# Cyber-Risiken.
# IT-gehackt.
# Gedeckt.

gewerbe
wittenbach
häggenschwil

**Frühlingsanlass – 4. Mai 2022**

**Eric Lehmann**
Senior Underwriter Technische Versicherungen
Versicherungsspezialist Cyber-Versicherungen

einfach. klar. helvetia
Ihre Schweizer Versicherung

# Die Frage ist nicht ob man gehackt wird, sondern wann?

# Top 10 Risiken weltweit

(Quelle - Allianz Risk Barometer 2022)

1. **Cyber Vorfälle** (Datendiebstahl / Erpressung / Spoofing / Bussgelder für Datenverstösse) – Vorjahr auf 
2. **Betriebsunterbrechung** (Brände / Naturkatastrophen / Unterbrechung der Lieferkette) – Vorjahr auf 
3. **Naturkatastrophen** (Sturm / Flut / Hochwasser / Erdbeben)
4. **Pandemie** – Vorjahr auf 
5. **Rechtliche Änderungen** (Sanktionen / Handelszölle / Protektionismus / Brexit)
6. **Klimawandel / Wetterkapriolen**
7. **Feuer / Explosion**
8. **Marktentwicklungen** (Stagnation / verstärkter Wettbewerb / M&A / neue Mitbewerber)
9. **Fachkräftemangel**
10. **Makroökonomische Entwicklungen**



helvetia
Ihre Schweizer Versicherung

# Wussten Sie das?

- **Cyberkriminalität** generiert global gesehen **mehr Geld als der Handel mit Drogen** (Hochschule Luzern 2022)
- **62% aller Opfer** von Cyberangriffen waren **KMU** (Varonis, Symantec, Cisco, Accenture & Ponemon Institute, 2018)
- **In ca. 70% der erfolgreichen Cybervorfälle** tragen **Mitarbeitende** des betroffenen Unternehmens zumindest eine **Mitschuld** (Nikolaus Stapels, 2019)
- **Ransomware-Angriffe** (Verschlüsselung von Daten) **wachsen** aktuell alleine in der CH rund **70% pro Quartal**
  **à** Ziel: Lösegeld erpressen (itmagazine.ch, 2020)
- **Pro Minute** werden **1'274 neue Schadprogramme** entwickelt (kaspersky, 2021)
- Die **durchschnittliche Schadenhöhe im KMU-Bereich** liegt bei rund CHF 80'000… (Nikolaus Stapels, 2020)
- KMUs investieren jährlich im Schnitt **weniger als CHF 500** für die **Cyber-Sicherheit**

# Cyberrisiken und die Methoden der Kriminellen.

# Cyber-Risiken?
# Beispiele von Cyber-Gefahren für Unternehmen

### Denial of Service (DoS)-Angriff
- Stillstand des Unternehmens **è** Systeme nicht mehr über Internet kommunikationsfähig
- Nicht mehr abrufbare/überlastete Website

### Interne Sabotagen eigener MA
- Datendiebstahl oder löschen von Daten
- Installation von Schadsoftware

### Trojaner / Ransomware / Malware
- Verschlüsselung von Daten
- Spionage von vertraulichen Daten
  **è** Datenschutzverletzung
- Zweckentfremdung der Systeme

### Phishing
- Spionage von Passwörtern
  **è** Zugriff auf Onlinebanking
- Manipulation der Website

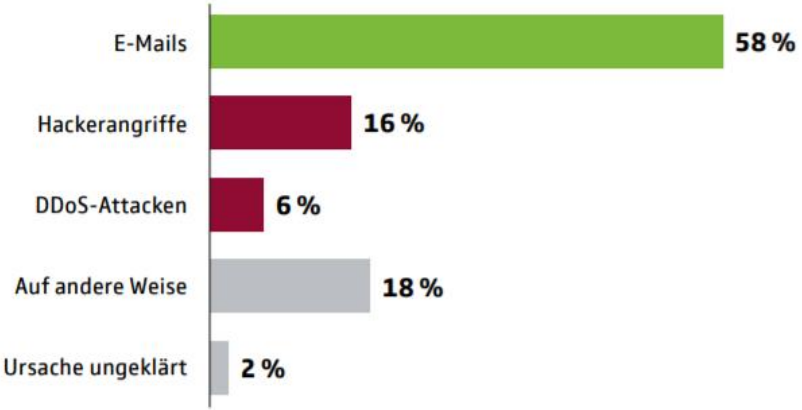
### Fahrlässig handelnder Mitarbeiter
- Versand vertraulicher Daten an falschen Empfänger


- **Vermögensschäden**
- **Reputationsschaden / Vertrauensverlust bei Kunden & Lieferanten**
- **Erpressungen**
- **Haftpflichtansprüche Dritter**

# Häufigste Einfallstore und ihre Schäden.

## Die Einfallstore

**Erfolgreiche Cyberangriffe erfolgten durch ...** [1]



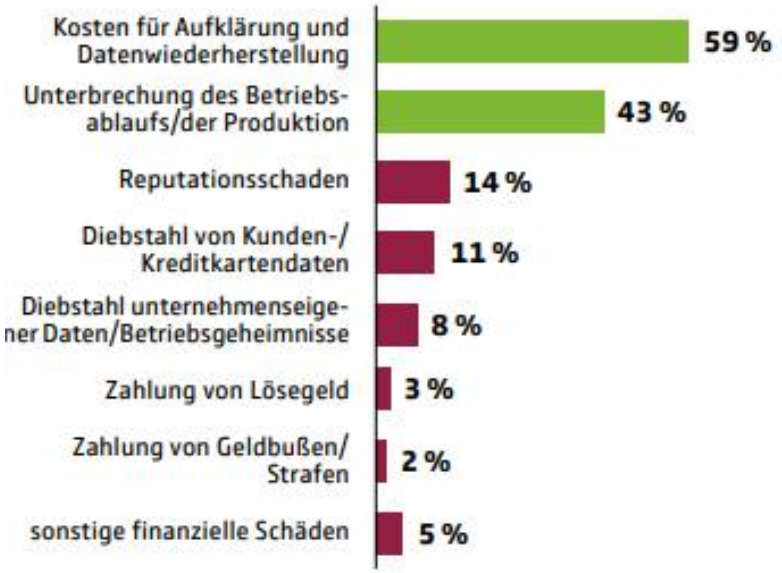

Quelle: Forsa

1 Mehrfachnennungen möglich

Quelle: GDV (2020). Forsa-Befragung. Cyberrisiken im Mittelstand

## Die Schäden

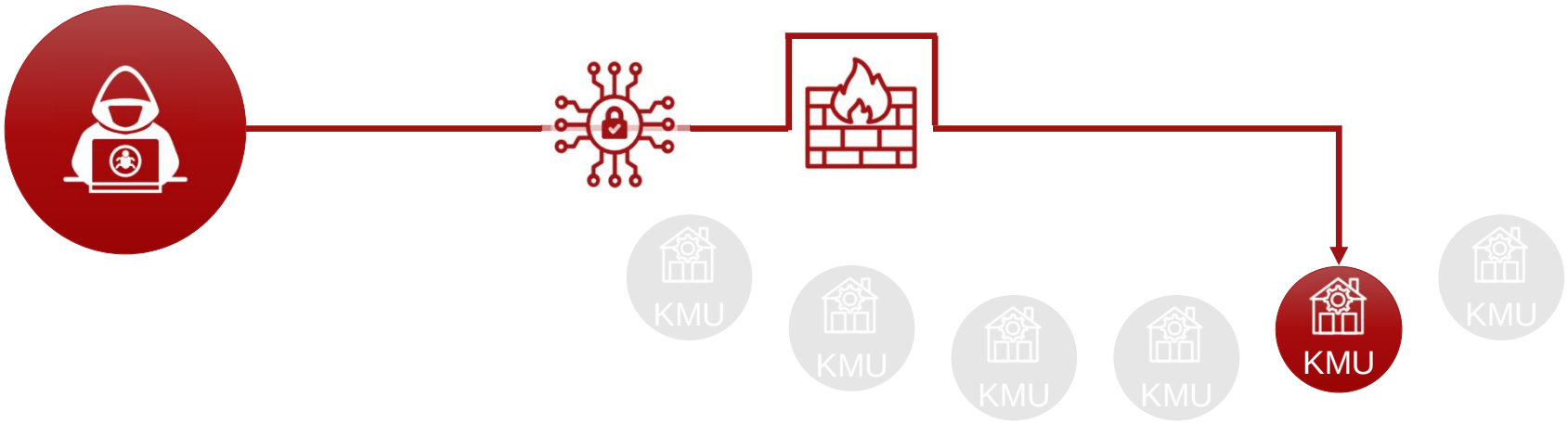
**Die Attacken führten zu wirtschaftlichen Schäden durch ...** [1]




Quelle: GDV (2018). Forsa-Befragung. Cyberrisiken im Mittelstand

helvetia
Ihre Schweizer Versicherung

# «Wer soll denn meine kleine Firma hacken.»



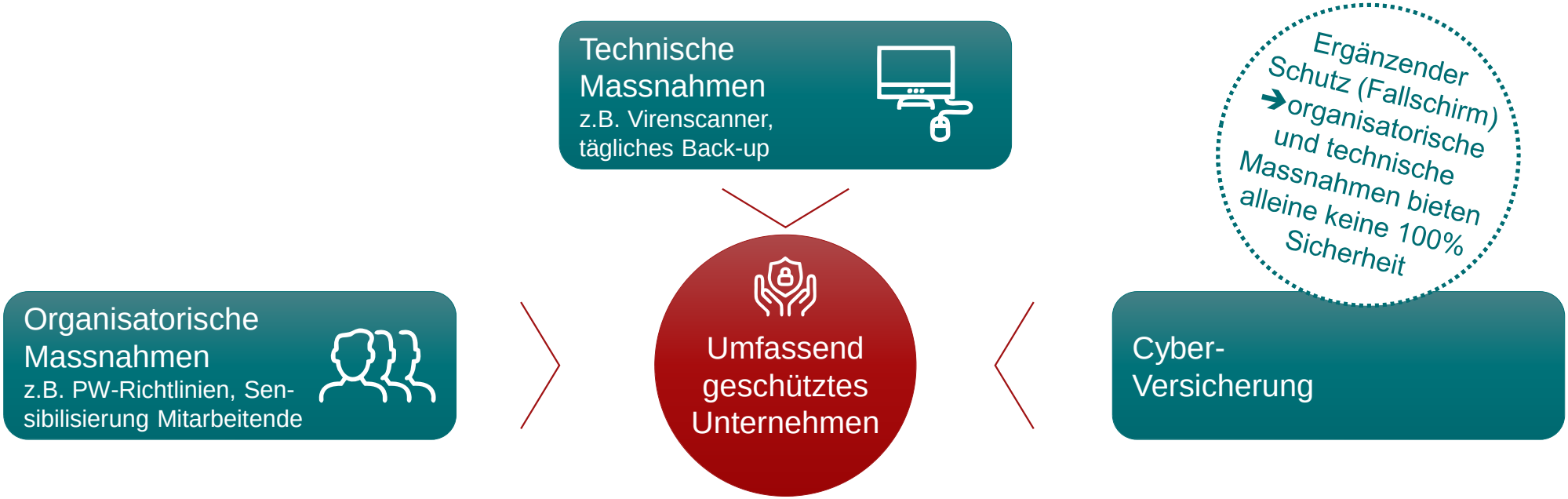

- Phishing Mail wird durch Klicken auf den Anhang geöffnet.
- Daraufhin wird eine Schad-Software nachgeladen.
- Diese umgeht die Firewall und die Antivirensoftware des Unternehmens.
- Ein Port am Router wird geöffnet – der Hacker hat Zugang zum Unternehmensnetzwerk.



helvetia
Ihre Schweizer Versicherung

# Schutz vor Cyber-Risiken.

# Wie schützt man sich vor Cyber-Risiken? Konkrete und greifbare Minimalanforderungen



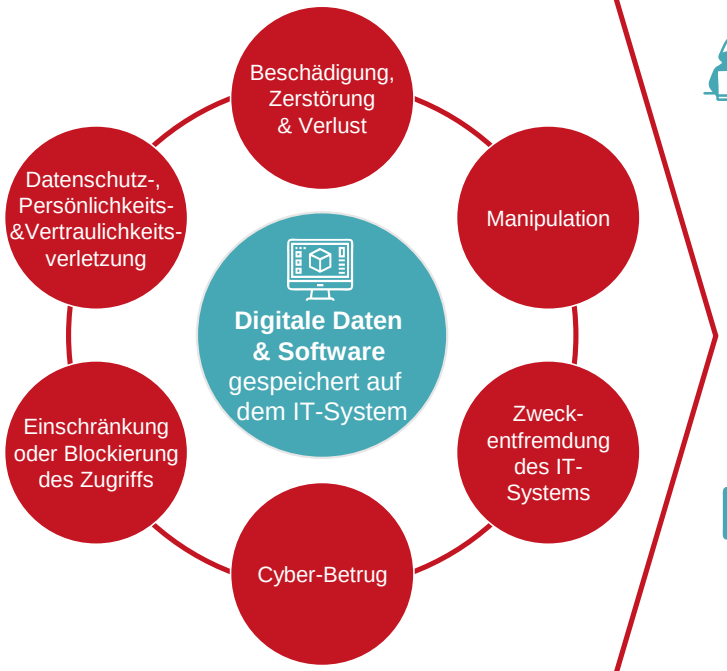

- "Grundhygiene" respektieren **è** NCSC (https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html)
- Im Eigeninteresse des Unternehmens soll der Sicherheitskatalog eingehalten werden



helvetia
Ihre Schweizer Versicherung

# Was deckt eine Cyber-Versicherung ab? Einfach auf einen Blick

## Versichert sind Cyber-Risiken...




## ...als Folge von

**Kriminellen Ursachen** wie

- interne Sabotage eigener Mitarbeitenden
- Ausnutzung der technischen System-/ Sicherheitsschwäche
- absichtliche oder unabsichtliche Installation/Ausführung schädlicher Software
- Installation/Einsatz unautorisierter Hardware
- Verwendung von gestohlenen Zugriffsinformationen
- DoS (Denial of Service)

**Nicht-kriminellen Ursachen** wie

- fahrlässige Bedienung durch eigene Mitarbeitende
- kurzzeitige Störungen

## mit kundenorientierten Leistungen für

**Eigenschäden**

**Haftpflichtschäden**

**Rechtsschutz**

helvetia
Ihre Schweizer Versicherung

# Übersicht der Leistungs-Pakete – für jedes Bedürfnis eine Lösung

| **Eigenschäden** (max. VS CHF 5 Mio./Leistungsdauer 12 Mt.) | LIGHT | STANDARD | PREMIUM | Sublimiten in CHF |
|---|---|---|---|---|
| Systemwiederherstellung | ü | ü | ü | |
| Datenrekonstruktion | ü | ü | ü | 30% max. 50'000 (Erhöhung Limiten möglich) |
| Mehrkosten zur Weiterführung der Datenverarbeitung | ü | ü | ü | |
| Gewinnausfall infolge Betriebsunterbruch | | ü | ü | |
| Schadensanalyse / Forensik | | ü | ü | |
| Notifikationsmanagement | | | ü | 250'000 für Disziplinar-, Aufsichts-, Verwaltungs-, Strafverfahren (nicht erhöhbar) |
| Reputationsmanagement | | | ü | |
| Lösegeldzahlung und Abwehr von Erpressung | | | ü | 30'000 für Lösegeldzahlung (Erhöhung der Limiten möglich) |
| Vermögensausgleich Cyber-Betrug / Manipulation | | | ü | 30'000 für finanzielle Transaktionen und Warenbestellungen (Erhöhung der Limiten möglich) |
| Mangelhafte Produktion | | (ü) | (ü) | |
| **Haftpflichtschäden** (max. VS CHF 5 Mio.) | LIGHT | STANDARD | PREMIUM | Sublimiten in CHF |
| Reine Vermögensschäden und immaterielle Schäden | | ü | ü | 100'000 für Ansprüche aus einer Vertragserfüllung infolge einer kriminellen Ursache (Erhöhung der Limiten möglich) |
| **Rechtsschutz** vertreten durch Coop Rechtsschutz (VS CHF 20'000) | LIGHT | STANDARD | PREMIUM | Sublimiten in CHF |
| Juristische Beratung und Erstintervention | | ü | ü | |



helvetia
Ihre Schweizer Versicherung

# Schaden-Beispiele

# Aufmerksam sein im Homeoffice.

**Cyberkriminelle haben rasch auf Corona-Pandemie reagiert. Sie nutzen Ängste und Unwissenheit aus:**

- Mehr betrügerische E-Mails und Phishing-Versuche.
- Zunahme von Spam-E-Mails über den E-Mail-Konten von Unternehmen.
- Starke Zunahme CEO-Fraud.

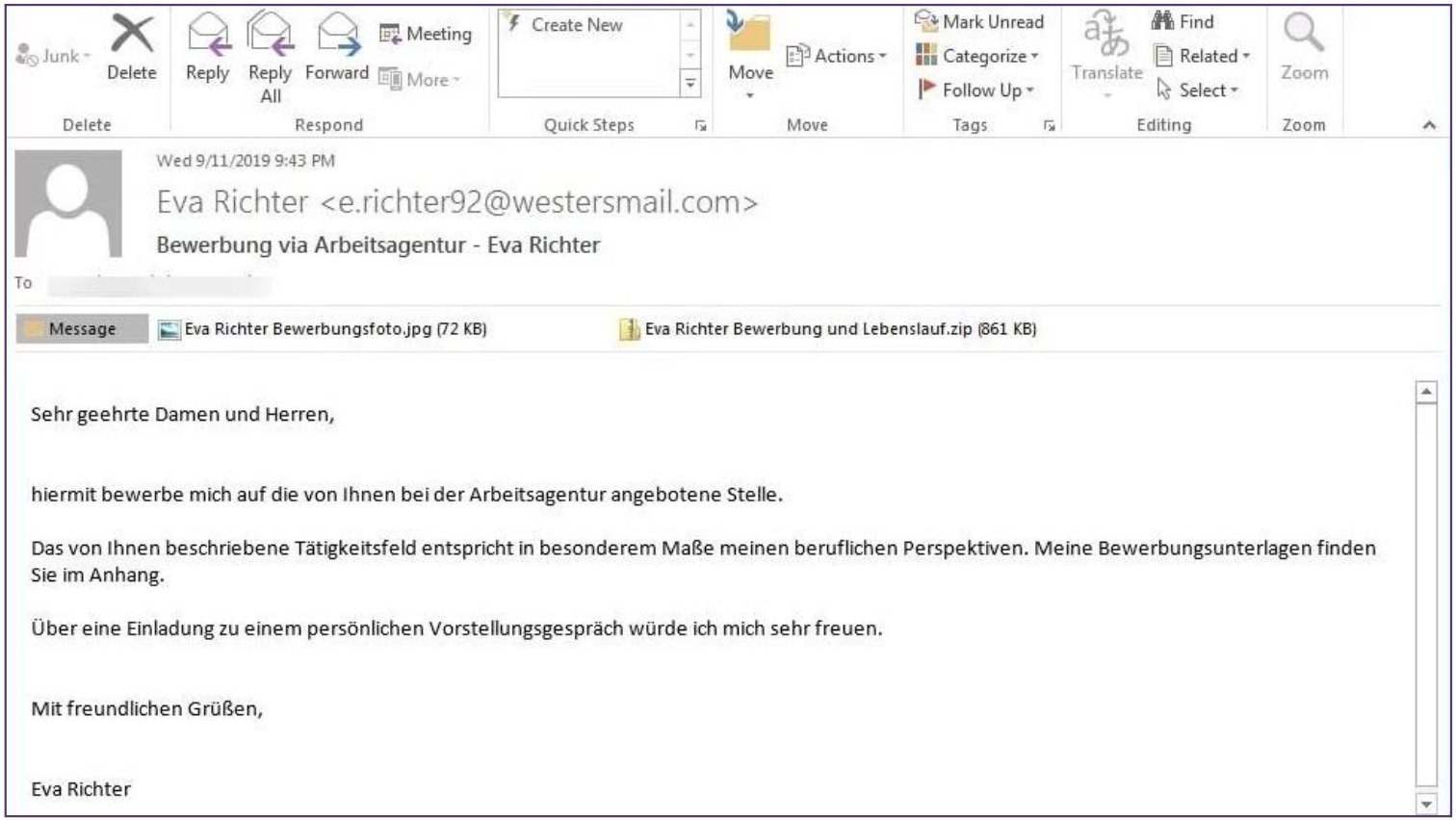
**Homeoffice wird zum neuen Einfallstor für Datendiebstahl:**

- Mangelhafte technische Infrastruktur
- Ungenügende Datensicherheit



helvetia
Ihre Schweizer Versicherung

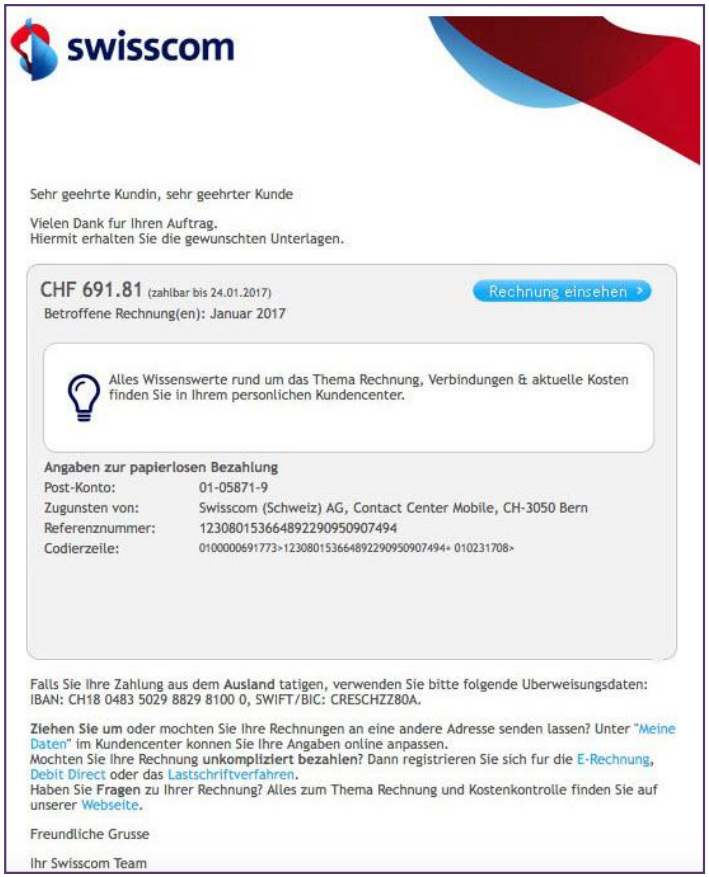
# Verschlüsselung von Daten.






helvetia
Ihre Schweizer Versicherung

# Manipulierte Rechnung.



swisscom

Sehr geehrte Kundin, sehr geehrter Kunde

Vielen Dank fur Ihren Auftrag.
Hiermit erhalten Sie die gewunschten Unterlagen.

CHF 691.81 (zahlbar bis 24.01.2017) Rechnung einsehen

Betroffene Rechnung(en): Januar 2017

Alles Wissenswerte rund um das Thema Rechnung, Verbindungen & aktuelle Kosten finden Sie in Ihrem personlichen Kundencenter.

**Angaben zur papierlosen Bezahlung**

| | |
|---|---|
| Post-Konto: | 01-05871-9 |
| Zugunsten von: | Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern |
| Referenznummer: | 123080153664892290950907494 |
| Codierzeile: | 0100000691773>123080153664892290950907494+ 010231708> |

Falls Sie Ihre Zahlung aus dem **Ausland** tatigen, verwenden Sie bitte folgende Uberweisungsdaten:
IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A.

**Ziehen Sie um** oder mochten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Mochten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich fur die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer Webseite.

Freundliche Grusse

Ihr Swisscom Team



helvetia
Ihre Schweizer Versicherung

# USB-Drop im Pausenraum – Aufschrift «Löhne der Geschäftsleitung».



helvetia
Ihre Schweizer Versicherung

# Cyber-Risiko: Verschlüsselung von Cloud-Daten

Eine versicherte Druckerei speichert viele ihre Daten auf einer Cloud. Einem Hacker gelang es, in diese Cloud einzudringen und mittels einer **Ransomware** alle darauf gespeicherten Daten zu verschlüsseln. Die Druckerei hatte anschliessend keine Möglichkeit mehr, auf ihre Daten zuzugreifen. Das Unternehmen stand dadurch während 4 Tage grösstenteils still. Neben der Verschlüsselung war auch nicht auszuschliessen, dass Daten gestohlen wurden.

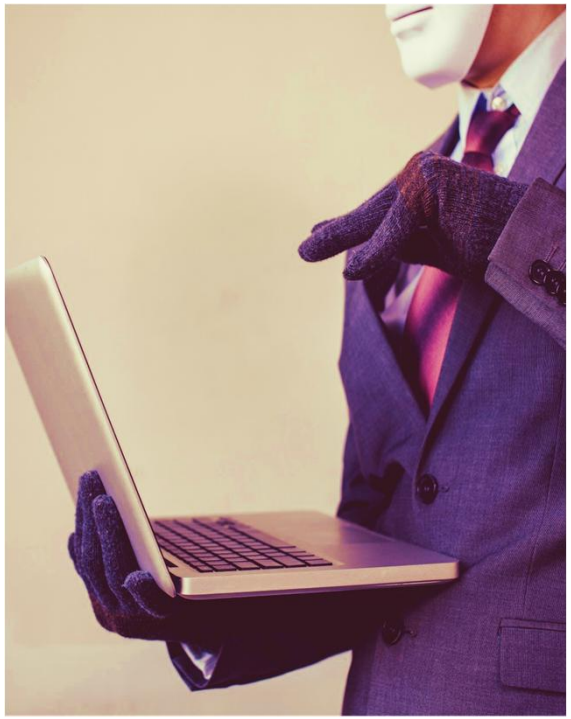
**Weil auch eine externe Cloud zum IT-System eines Unternehmens gehört, übernimmt Helvetia die daraus entstehenden Kosten wie**

- die Wiederherstellung der Daten beim Versicherungsnehmer
- der manuellen Rekonstruktion derjenigen Daten, die technisch nicht mehr über das Back-up der Cloud wiederhergestellt werden können
- den Gewinnausfall aufgrund des Betriebsunterbruchs

**Helvetia und ihr juristischer Partner betreut die Druckerei zudem in den rechtlichen Fragen betreffend Datenschutz, die durch einen solchen Vorfall aufkommen können.**

helvetia
Ihre Schweizer Versicherung

# Cyber-Risiko: Betrug durch Vorspiegelung einer falschen Identität



Der Buchhalter einer Werbeagentur erhielt eine E-Mail von seinem angeblichen CEO (**Fake President Fraud**). Der Betrüger behauptete, dass es sich um eine streng vertrauliche Angelegenheit (Kauf eines Unternehmens im Ausland) handelt und niemand sonst darüber informiert werden darf. Der Auftrag lautete: „Bitte veranlasse schnellstmöglich eine Überweisungen auf unten erwähntes Konto, damit der Unternehmenskauf erfolgreich realisiert werden kann“ Der Buchalter tätigte diese Überweisung. Einige Tage später traf der Buchalter den Chef zufällig und sprach ihn auf die Transaktion an. Erst dann fiel der Betrug auf. Der CEO war zwar wirklich für Geschäfte im Ausland, jedoch hat er eine solche Überweisung nie in Auftrag gegeben.

**Gemeinsam mit der Bank wird versucht, das falsch überwiesene Geld wieder zurückzuholen. Falls dies nicht gelingt, übernimmt Helvetia die entstandenen finanziellen Verluste.**



helvetia
Ihre Schweizer Versicherung

# Cyber-Risiko: Umleitung von Zahlungsströmen

Ein Betrüger spionierte die E-Mail-Kommunikation von einer Garage mit einem Geschäftspartner aus. Im Anschluss gab sich der Betrüger für den Geschäftspartner aus und verwendete dabei eine ähnliche Kommunikation mit gleicher Anrede und gleichem Schlusssatz, wie dies der Geschäftspartner immer macht. Die konkrete Betrugsstrategie: Der Betrüger teilte der Garage mit, dass sich eine Bankverbindung geändert hat, die für alle künftigen Zahlungen gilt. Die Garage überwies die nächste Zahlung an die neue Bankverbindung, denn es gab keinen Anlass, an der Seriosität dieser Information zu zweifeln. Erst mit der Zahlungserinnerung des „echten“ Geschäftspartners flog der Betrug auf. Und das Geld? War natürlich längst verschwunden. (**Payment Diversion**)

**Helvetia übernimmt den Vermögensschaden der Garage. Zudem ist anzunehmen, dass für die Spionage eine Malware auf dem System installiert wurde. Diese wird mittels einer Schadenanalyse durch einen unserer IT-Security-Partner eruiert und entfernt.**



helvetia
Ihre Schweizer Versicherung

# Cyber-Risiko: Maschinen-Steuerung (OT) gehackt

Ein Betrüger gab sich am Telefon als Systemadministrator eines Autoteileherstellers aus und versuchte so an Benutzernamen und Passwörter von Mitarbeitenden zu gelangen (**Social Engineering**). Durch das Vortäuschen von Betriebskenntnissen (Namen von Vorgesetzen, Arbeitsabläufen, Maschinentypen usw.) wurde das Vertrauen eines Mitarbeitenden gewonnen, wodurch dieser die gewünschten Informationen anschliessend preis gab. Mit diesen Daten war es dem Betrüger möglich, in das Maschinennetzwerk der Firma einzudringen. Dort veränderte er einige Parameter an der Steuerung. Da die Manipulation nicht sofort bemerkt wurde, entstand eine fehlerhafte Produktionsreihe.

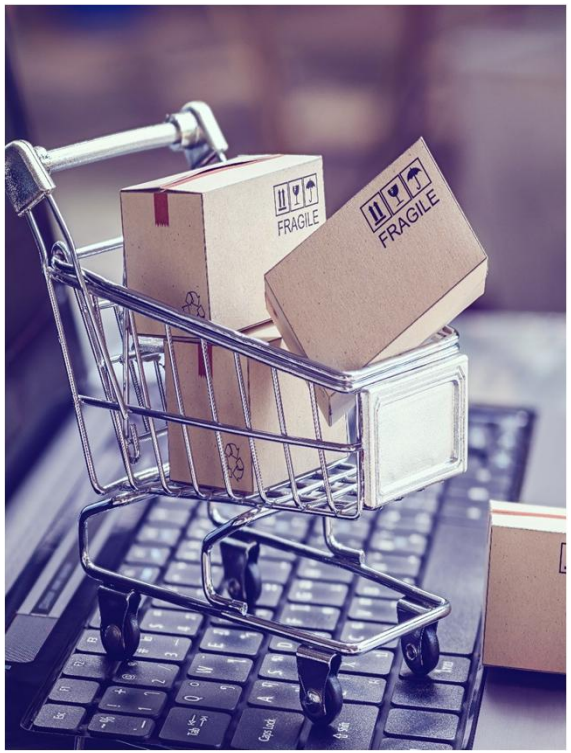
**Helvetia kommt für folgende Kosten auf:**

- Aufwendungen für die Analyse des Schadens und die Wiederherstellung der korrekten Parametrisierung
- Vermögensschaden (Entsorgung der fehlerhaften Produkte und Neuproduktion) aufgrund der mangelhaften Produktionsserie



helvetia
Ihre Schweizer Versicherung

# Cyber-Risiko: Online-Shop lahmgelegt




Während der ertragsreichen Weihnachtszeit wurde der Online-Geschenke-Shop einer unserer Versicherungsnehmer mittels einer **DoS-Attacke** angegriffen, wodurch die Kundinnen und Kunden nicht mehr auf die Website zugreifen konnten. Bald darauf kam eine Mail mit einer Erpressungsforderung über CHF 10'000 und dem Versprechen, dass der Angriff solange anhalte, bis das Geld überwiesen sei.

**Nach einer kurzen Schadenanalyse leitet ein Partnerunternehmen von Helvetia mittels eines Geo-Filters den 'falschen' Datenverkehr um und bringt den Onlineshop dadurch wieder zum Laufen, ohne dass die Erpressung gezahlt werden muss. Die Aufwendungen für diese Notfallmassnahme übernimmt die Helvetia. Zudem erhält der Versicherungsnehmer Inputs, wie er sich in Zukunft gegen DoS Attacken noch besser aufstellen kann. (z.B. mit einer Disaster Recovery Site)**
**Helvetia kommt zudem für die Kosten eines externen Kommunikationsberaters auf, um den guten Ruf bei den Kundinnen und Kunden zu schützen und um aktive Schadensbegrenzung zu betreiben.**

helvetia
Ihre Schweizer Versicherung

# Praktische Links

- Nationales Zentrum für Cybersicherheit (NCSC) **è** https://www.ncsc.admin.ch/ncsc/de/home.html
- Kaspersky Cyberthreat-Echtzeitkarte **è** https://cybermap.kaspersky.com/de
- SWISSCYBER SECURITY.NET **è** https://www.swisscybersecurity.net/
- CYBERSAFE **è** https://www.cyber-safe.ch/de/willkommen/
- Schweizerische Kriminalprävention **è** https://www.skppsc.ch/de/