Cyber Risiken – für Immobilienberufe (k)ein Thema?

Online-Event SVIT
vom 18. Oktober 2021

Thomas Greub, AXA Versicherungen AG, Oktober 2021

Agenda

max. 45 Min.

1. Überblick	1. Cyberkriminalität 2. Aktuelle Situation
2. Cyberangebote von AXA	1. Cyberversicherung 2. Präventionsservice
3. Zusammenfassung und Fragen	

1

Überblick

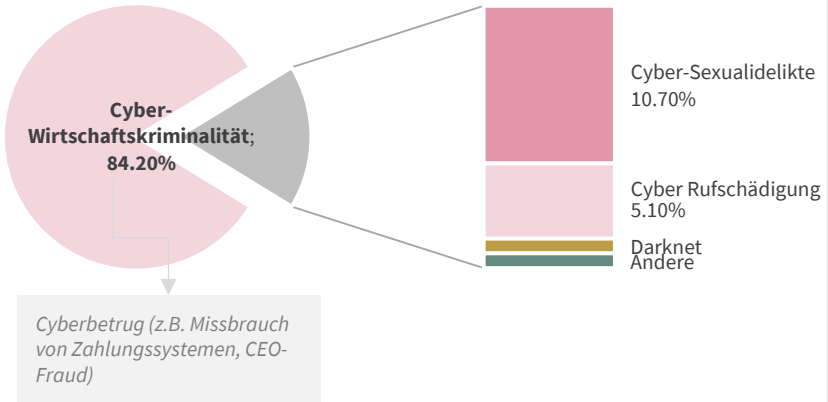
1.1

Cyberkriminalität

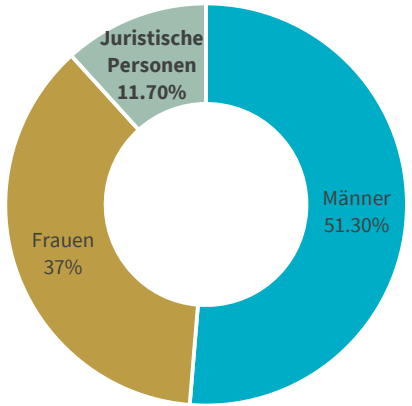
Cyberkriminalität (digitale Kriminalität)

2020 wurden 24’398 Straftaten mit einer digitalen Komponente registriert (man rechnet mit einer hohen Dunkelziffer)

Bereiche der Cyberkriminalität



Geschädigte



Quelle: Polizeiliche Kriminalstatistik, Jahresbericht 2020, Neuenburg 2021

1.2

Aktuelle Situation

Was IT-Security-Experten den Schlaf raubt

Cyberkriminelle nutzen Coronavirus und BAG-Logo, um Malware zu verbreiten

Auto AG fährt Systeme nach Hackerattacke wieder hoch

Luzerner Zeitung

Nach der Egolzwiler Meier Tobler ist auch die Rothenburger Auto AG Group von Hackern angegriffen worden. Die IT-Experten des Bundes geben Tipps, wie sich KMU schützen können.

Cyberangriff legt Zürcher Firma lahm

Attacken auf IT-Systeme nehmen zu. Nun hat es die Firma Meier Tobler aus Schwerzenbach erwischt.

Zürcher IT-Firma von Hackerangriff betroffen - Attacke weitet sich aus

Die Firma Crealogix entwickelt IT-Systeme für Banken, nun wurde sie Opfer von Hackern. Jetzt warnen die Behörden vor landesweiten Angriffen.

NEWS

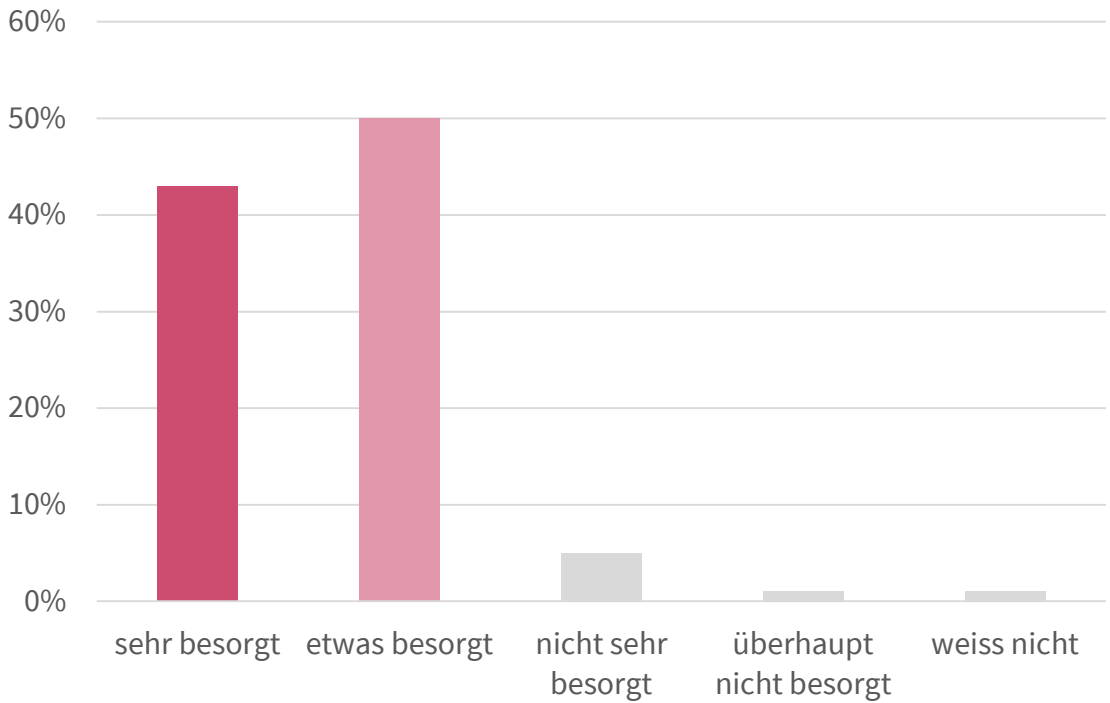
Nach Ransomware-Angriff

Uster rüstet sich gegen Cyberangriffe

Do 10.10.2019 - 10:55 Uhr
von René Jaun

Die Stadt Uster schaft eine neue Stelle zur Bekämpfung von Cyberkriminalität. Der Schritt erfolgt als Konsequenz auf einen Ransomware-Angriff im Dezember 2018. Zwar gingen damals keine wichtigen Daten verloren, doch der Fall kostete die Stadt einen beträchtlichen Betrag.

Wie besorgt sind Sie über Cyberbedrohungen?



Quelle: Umfrage PwC bei 111 CEO in der Schweiz, März 2021

Unternehmensziel: Informationssicherheit

Klären, was geschützt werden soll

Geistiges Eigentum
Wettbewerbsvorsprung

Datenschutz
Kundenvertrauen

Rechtssicherheit
Haftung der Geschäftsführung

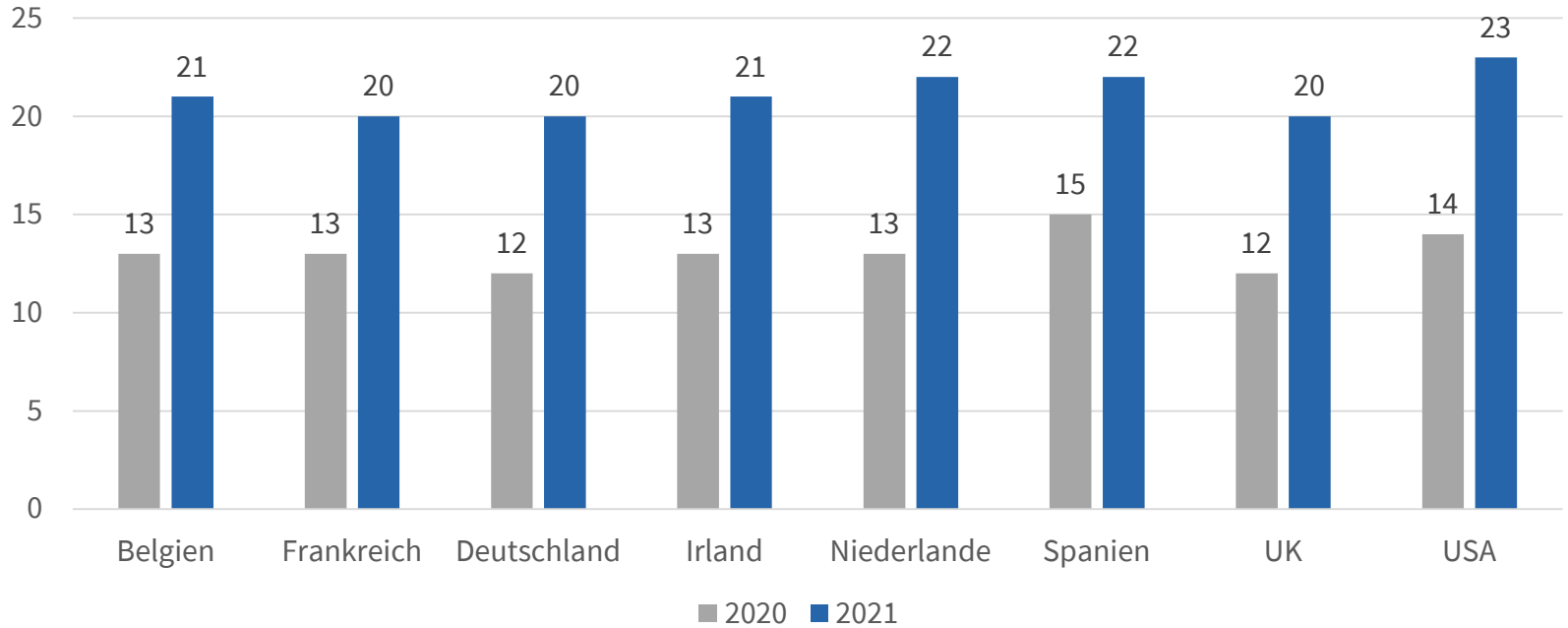
Schaden verhüten
Kosten reduzieren

Lieferfähigkeit
Verfügbarkeit der Waren

Festlegung
Risikoziele

Wieviel Geld wird für Cyber-Security ausgegeben?

Anteil Cyber Security Kosten im Verhältnis zu den gesamten IT Kosten (in %)

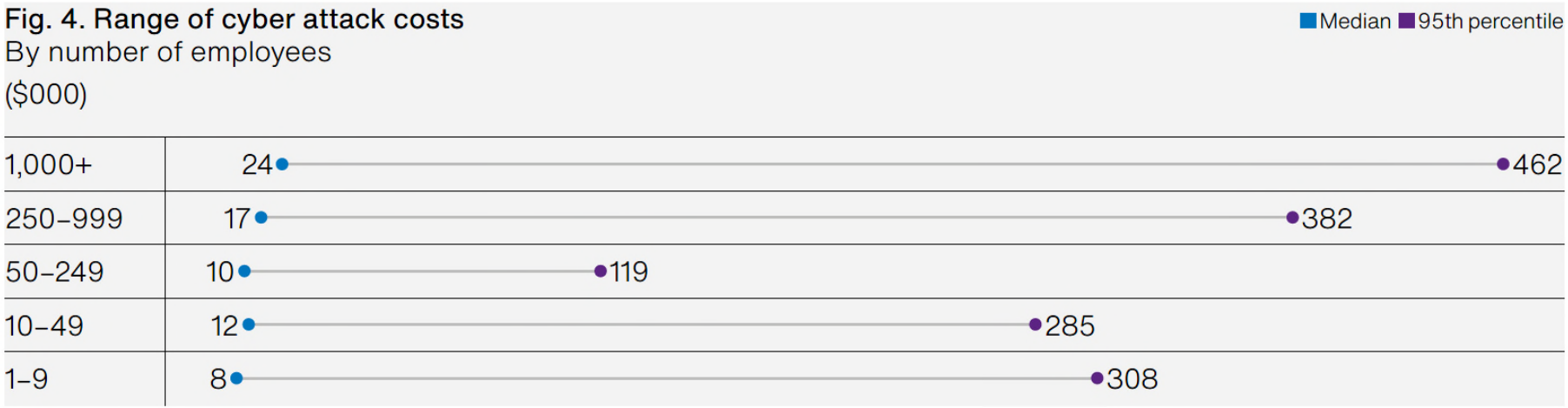


6,042 organisations across eight countries by size and sector (1,000 plus each from the USA, UK, France and Germany; more than 500 each from Belgium, Spain and The Netherlands; and 300 plus from the Republic of Ireland)
Respondents completed the online survey between 5 November 2020 and 8 January 2021

Quelle: Hiscox, Cyber Readiness Report 2021

Welche Schadenhöhen sind zu verzeichnen?

Fig. 4. Range of cyber attack costs
By number of employees
($000)



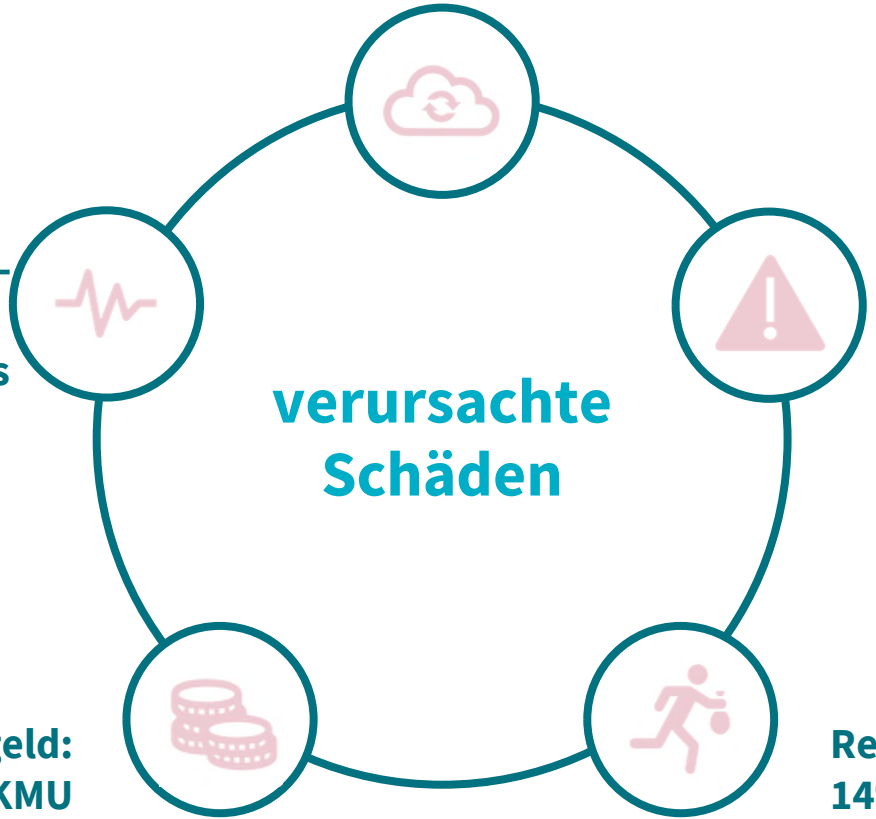
- Median bedeutet, dass 50% kleiner und 50% grösser sind als der Messwert.
- 95%-Perzentil bedeutet, dass 95% kleiner oder gleich gross sind wie der Messwert.

Quelle: Hiscox, Cyber Readiness Report 2021

Datenwiederherstellung:
59% betroffene KMU

Betriebsunterbruch:
43% betroffene KMU

- **35% konnten die Systeme am ersten Tag wieder-herstellen**
- **42% brauchten bis drei Tage**
- **23% benötigten mehr als 3 Tage**



Diebstahl von Daten:
19% betroffene KMU

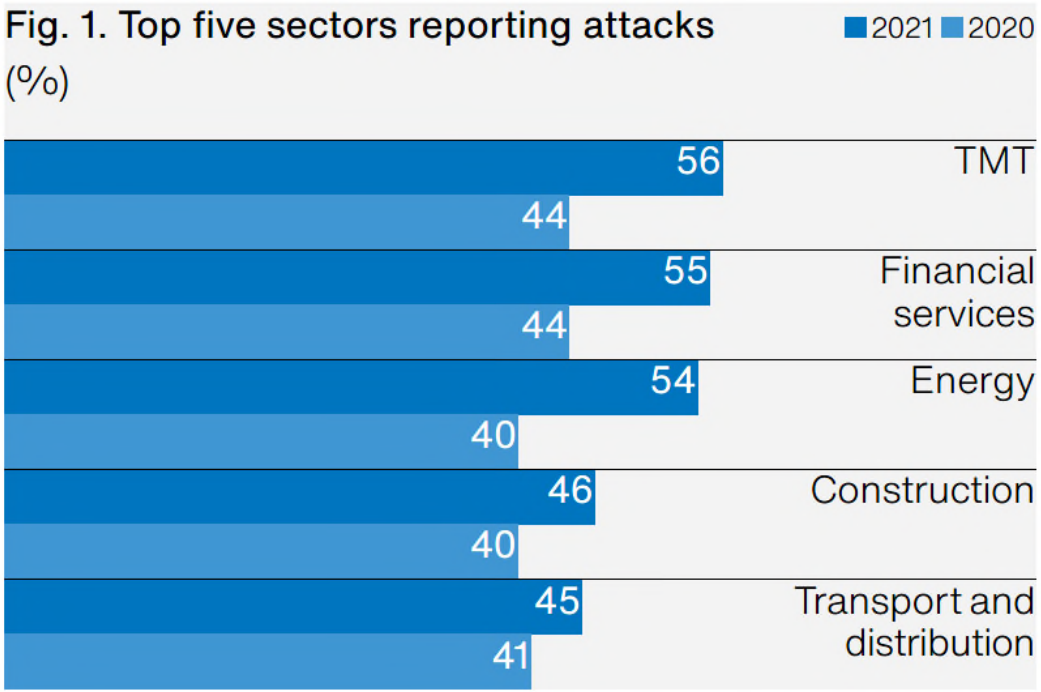
Zahlung von Lösegeld:
3% betroffene KMU

Reputationsschaden:
14% betroffene KMU

Quellen: Cyberrisiken im Mittelstand, Studie GDV, 2018/2020; Mehrfachnennungen möglich

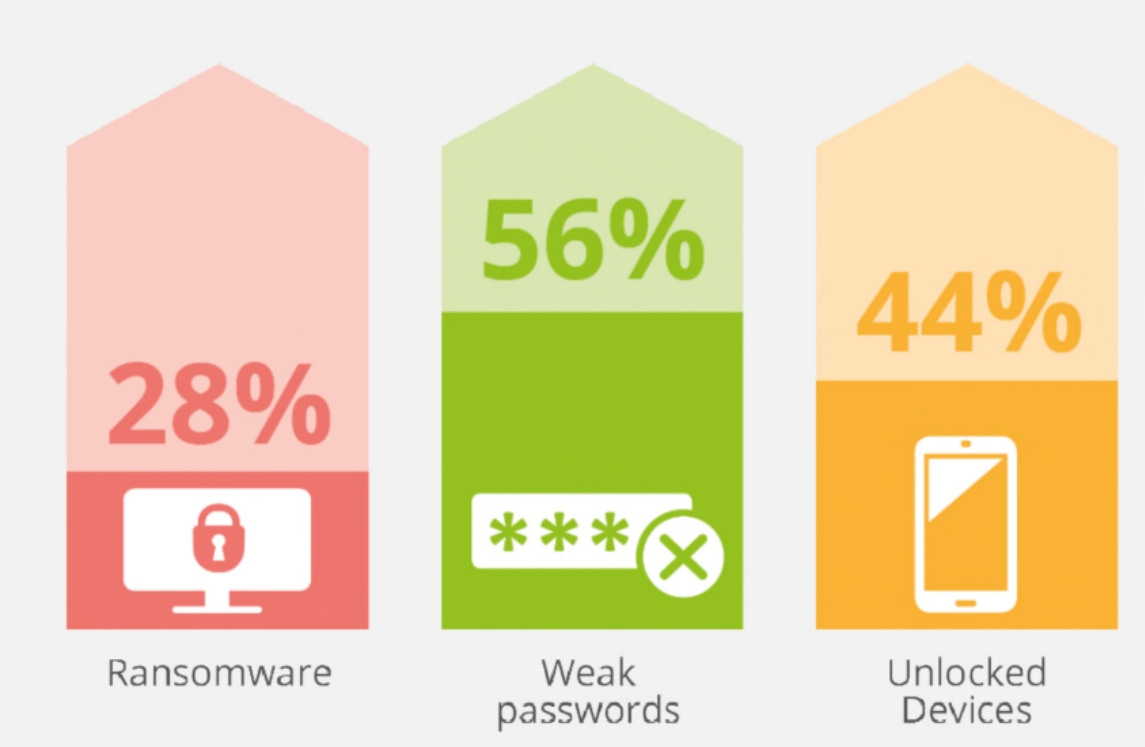
Welche Branchen werden hauptsächlich angegriffen?

TMT bedeutet: technology, media and telecoms



Quelle: Hiscox, Cyber Readiness Report 2021

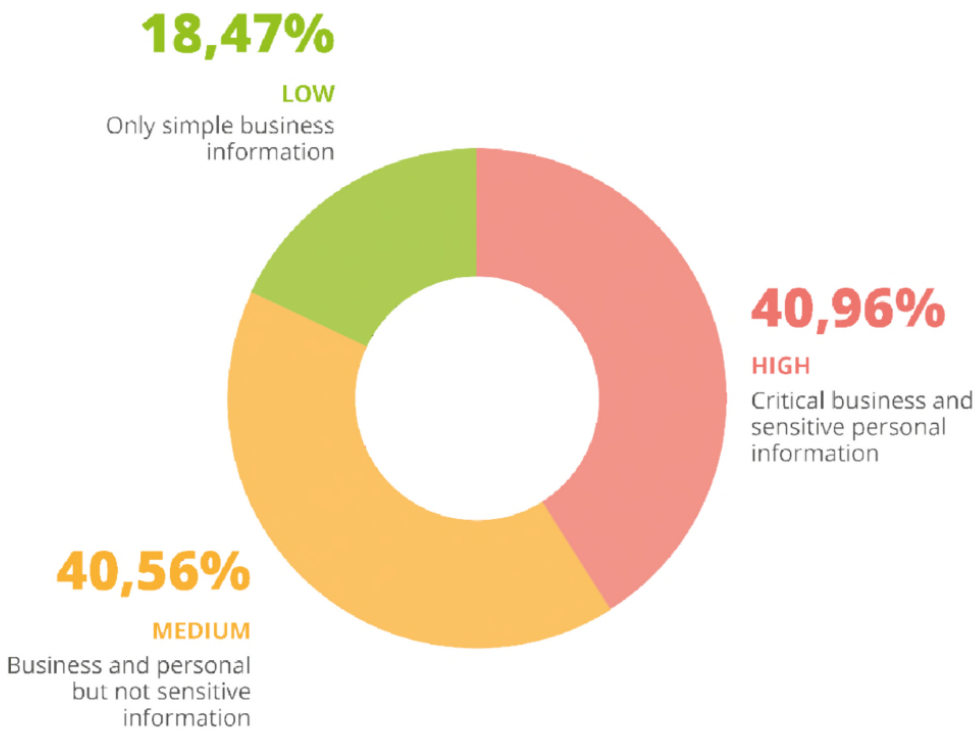
Wie dringen die Kriminellen ein?



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

Welche Daten haben KMU?

Weshalb werden KMU vermehrt zur Zielscheibe der Cyberkriminellen?



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

Was sind die häufigsten Cybersecurity Vorfälle?

Kriminelle greifen nicht nur grosse Unternehmen an – im Gegenteil!

Angegriffene Unternehmen

IT-Dienstleister wurden mit Ransomware attackiert (dies gilt v.a. für Unternehmen mit weniger als 50 Mitarbeiter), da diese Firmen im Homeoffice oft nicht gut genug geschützt sind. Der Zugriff erfolgt via das Microsoft Remote Desktop Protocol (RDP). Ein VPN ist oft nicht vorhanden.

Was kann man dagegen tun:

- Einsatz eines VPN (hier gibt es auch grosse Unterschiede!)
- Backup, welche mindestens wöchentlich offline gemacht werden
- Mitarbeitertraining v.a. für den Gebrauch von Passwörtern und der Erkennung von Phishing

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

Was sind die häufigsten Cybersecurity Vorfälle?

Kriminelle greifen nicht nur grosse Unternehmen an – im Gegenteil!

Angegriffene Unternehmen

Rechtsanwaltskanzleien mit weniger als 25 Angestellten, wobei im Homeoffice der Gebrauch von eigenen Computern zulässig war. Hier kam es wiederholt zum Diebstahl von Laptops mit sensitiven Klientendaten.

Was kann man dagegen tun:

- Einschränkung des Zugriffs auf Daten, welche für den Job gebraucht werden
- Verschlüsselung der Daten von allen Geräten
- Schulung der Mitarbeiter im Umgang mit Laptops und wie Daten geschützt werden können

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

Was sind die häufigsten Cybersecurity Vorfälle?

Kriminelle greifen nicht nur grosse Unternehmen an – im Gegenteil!

Angegriffene Unternehmen

Bei Webshops mit weniger als 25 Angestellten wurden oft E-Mail-Accounts mit Phishing attackiert. Sobald der Mitarbeiter hier unvorsichtig handelte, wurde der E-Mail-Account von den Kriminellen übernommen. Es wurden dann E-Mails an Kunden verschickt, wo man diesen auf geänderte Bankkonten aufmerksam macht. Wenn der Mitarbeiter auf den Link klickt, wird er nach User-Informationen und dem Passwort gefragt.

Was kann man dagegen tun:

- Es braucht für alle Plattformen Multi-Faktoren-Authentifizierung
- Mitarbeitertraining gegen Phishing
- Einführung von Passwörtern, welche nicht einfach zu knacken sind

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

Was sind die häufigsten Cybersecurity Vorfälle?

Kriminelle greifen nicht nur grosse Unternehmen an – im Gegenteil!

Angegriffene Unternehmen

Freizeit und Sportclubs mit weniger als 75 Angestellten werden oft mit Ransomware angegriffen. In bekannten Fällen kam zum Vorschein, dass die Anti-Virus-Software nicht aktuell war.

Was kann man dagegen tun:

- Sicher stellen, dass alle Software dem aktuellen Stand entsprechen Dies gilt v.a. auch für die Anti-Virus-Software
- Installation eines Spam und Virus-Filters bei E-Mail
- Offline Backups mindestens wöchentlich machen
- Mitarbeitertraining zur Erkennung von Phishing

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

Was sind die häufigsten Cybersecurity Vorfälle?

Kriminelle greifen nicht nur grosse Unternehmen an – im Gegenteil!

Angegriffene Unternehmen

Technologieunternehmen mit weniger als 75 Mitarbeitern sind oft von CEO Fraud betroffen. Dabei geht es z.B. darum, dass von einem gehackten E-Mail-Account des CEO nach einer schnellen Zahlung verlangt wird.

Was kann man dagegen tun:

- Sicherstellen, dass sich alle Mitarbeiter an Weisungen und Prozesse halten
- Rückbestätigungen haben über einen anderen Kanal zu erfolgen (z.B. Telefon)

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

“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%
mein Unternehmen ist zu klein

81%
unsere Computersysteme sind umfassend geschützt

58%
wir waren noch nie Opfer einer Cyberattacke

70%
unsere Daten sind nicht interessant

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

Was sind typische Risiken in der Immobilienbranche

Haftpflicht als Hauptrisiko

Hauptrisiko in der Haftpflicht:

- Zugriffe auf fremde Bankkonten (z.B. bei STWEG oder Verwaltungsmandaten)
- Viele elektronische Kontakte, was die Verbreitungsmöglichkeiten und mögliche Haftpflichtansprüche bei unwissentlicher Verbreitung von Viren, Trojaner erhöht
- Grosse Verantwortungen bei Immobilienverkäufen (Immobilienmaklern); grosse Auswirkungen, wenn Immo-Verkaufsprozess gestört wird
- Vielzahl von Rechnungsstellern, infolge Bewirtschaftung der Liegenschaften und Bezahlung der anfallenden Rechnungen (Social Engineering)

Hauptrisiken bei Eigenschäden

- hohe Abhängigkeit von der IT
- Vielzahl von elektronischen Kontakten (z.B. Schadsoftware innerhalb einer Wohnungsbewerbung) und der damit verbundenen Schwierigkeit die Schadsoftware zu erkennen
- hoher Bedarf für den Präventionsservice (Mitarbeitertraining und IT-Security-Plattform)

2

Angebote der AXA

Unsere Angebote im Überblick

AXA bietet Lösungen auf allen drei Verteidigungslinien

Cyber Check & Schutz für KMU

Präventionsservice

Technische Massnahmen

- Monatlicher IT-Sicherheitsbericht
- Handlungsempfehlungen, um Systeme sicherer zu machen
- Proaktive Information über aktuelle Gefahren

Organisatorische Massnahmen

- Mitarbeiter Security-Trainings
- Learnvideos und Checklisten
- Notfallplan, um auf Vorfälle bestmöglich vorbereitet zu sein

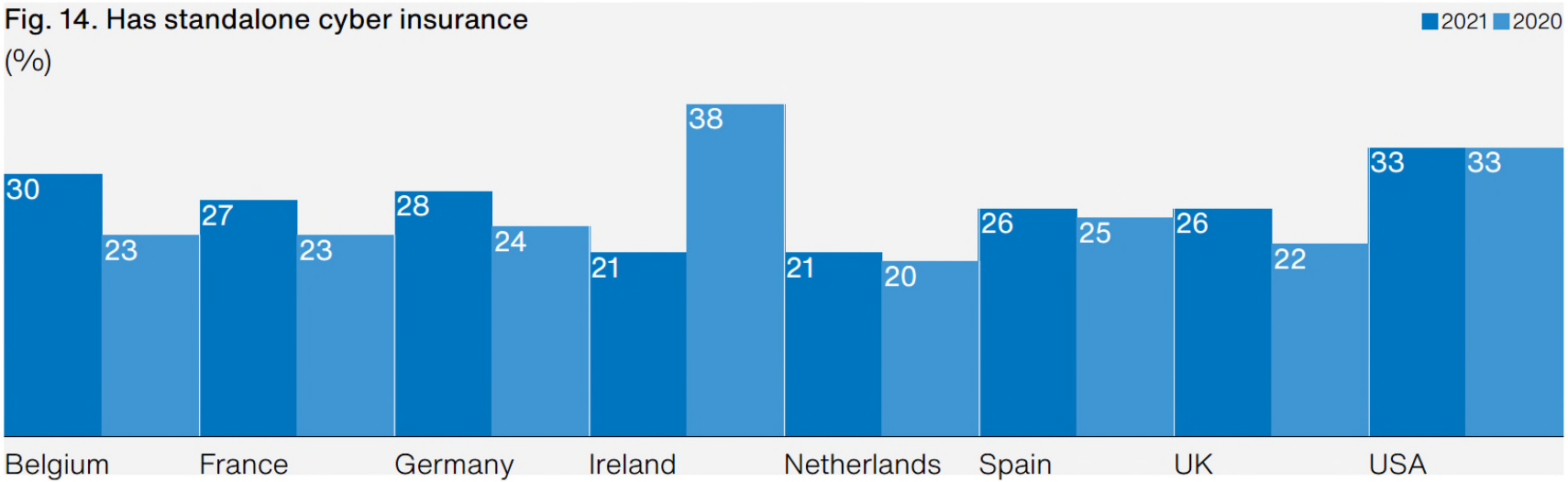
Versicherung

- Risikotransfer
- Soforthilfe 24/7 und Schadenmanagement
- Unterstützung Risk Management
- Expertennetzwerk

2.1

Cyberversicherung

Wie verbreitet ist die Cyberversicherung?



Wie viele KMU haben in der Schweiz eine Cyberversicherung?
Gemäss einer Studie der Mobiliar u.a. (Dezember 2020) sollen dies 16% der KMU (4-49 Mitarbeiter) sein.

Quelle: Hiscox, Cyber Readiness Report 2021

Produktübersicht Cyberversicherung

Grunddeckung

Eigenschäden (inkl. Betriebsunterbruch)	Haftpflichtschäden	Krisenmanagement
Eigene Daten auf eigener IT oder in einem Cloud-System	Daten von Dritten	Sofortmassnahmen, Kosten für Krisenberatung und –kommunikation

Zusatzdeckungen

Online Banking	Social Engineering	Telefon Hacking	Zahlungen Lösegeld

Cyberversicherung

Schadenbeispiel: Erpressungstrojaner: Diesen Fall kann jede Unternehmung betreffen!

Ein **Erpressungstrojaner** ist über den **E-Mail-Anhang** einer Stellenbewerbung ins IT-System gelangt.

Das **installierte Security Programm** erkannte den Trojaner nicht.

- **Verschlüsselung** aller Server- und Adressdatenbanken
- Keine Anmeldung der Arbeitsstationen mehr möglich
- **Lösegeldforderung** in Form von Bitcoins
- Entscheid mit Polizei und Staatsanwaltschaft kein Lösegeld zu bezahlen.

× Datensicherung auf NAS (netzgebundener Speicher) wurde ebenfalls verschlüsselt

✓ Regelmässige Datensicherung auf externer Harddisk

Schadenprozess

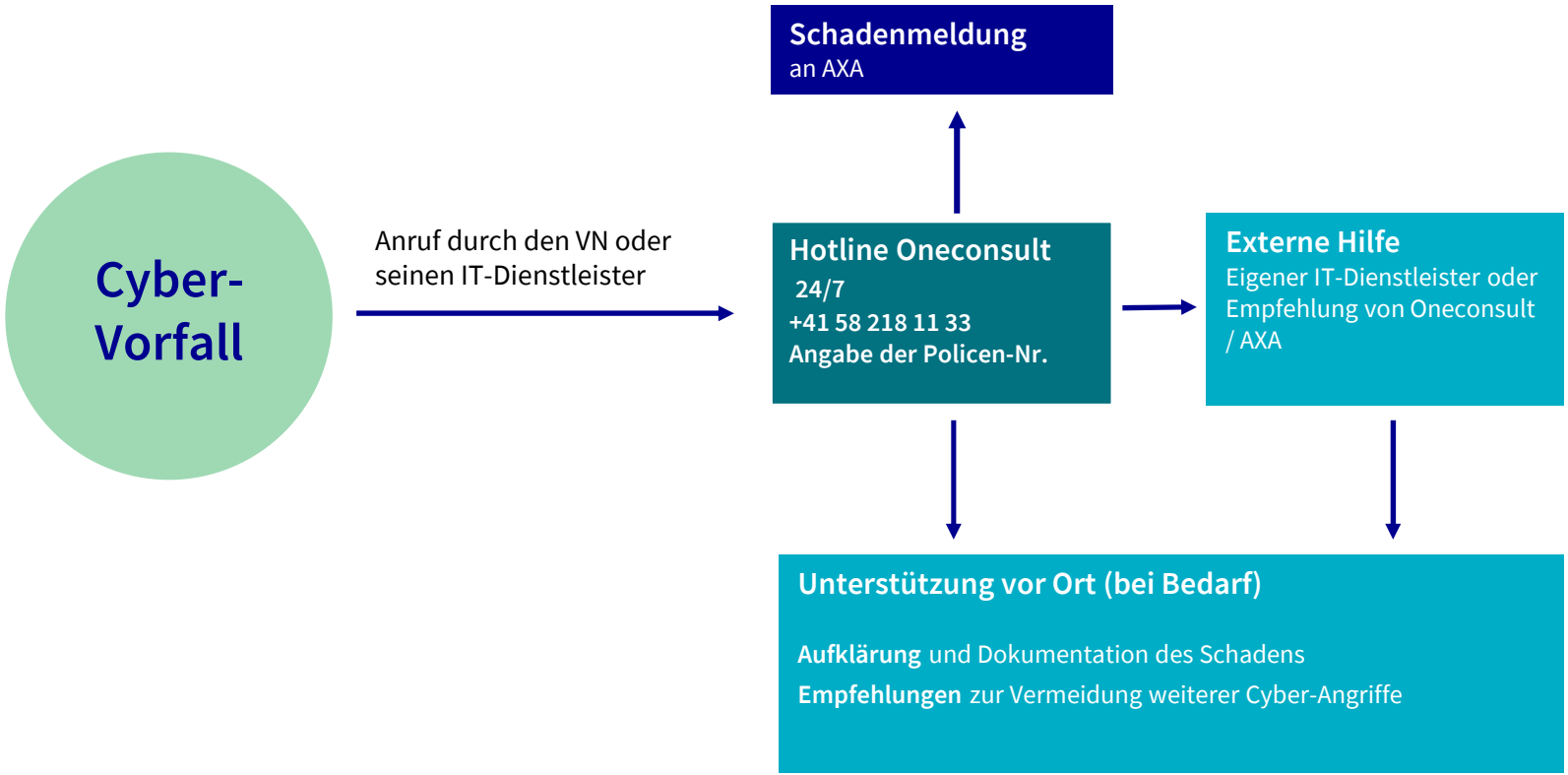
- Anruf bei der Soforthilfe 24/7 bei Oneconsult
- Bewertung der bisherigen Massnahmen durch Experten
- Empfehlung von Sofortmassnahmen
  - Weitere telefonische bzw. vor Ort Unterstützung
  - Krisenmanagement mit Experten-Netzwerk (Anwälte, PR, …)

Entschädigung

Neuinstallation Server und PC	CHF 15’000
abzgl. Mehraufwand für neue Hardware	CHF -2’000
Betriebsunterbrechungsschäden	CHF 10’000
Aufrechterhaltung des Betriebs	CHF 5’000
Datenwiederherstellung ab Backup und Urbelegen	CHF 3’000
abzgl. Selbstbehalt	CHF -2’000
Total Netto Entschädigung	**CHF 29’000**

Der Schadenmeldeprozess

Verhalten im Schadenfall



Was kann man aus Schäden lernen?

Anforderungen der Versicherung an den Kunden

Backup, Backup,
Backup!

Schadenarten und –ursachen sind **vielfältig**

Obliegenheiten prüfen
vorab mit Kunden klären!

Besser auf den Schaden vorbereiten – **Notfallplanung**!

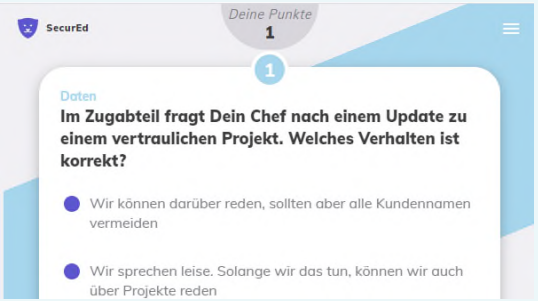
Nicht an der falschen Stelle sparen (IT-Security)!

2.2

Präventionsservice

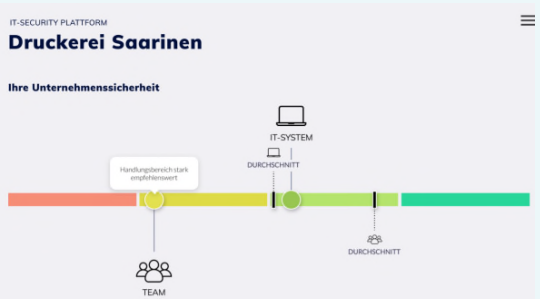
Präventionsservice

Ist seit 1. Juli 2020 im Einsatz



Schulungs-Plattform
Cyber-Training für Geschäftsführende und Mitarbeitende über die Gefahren im Internet. Dieses beinhaltet:

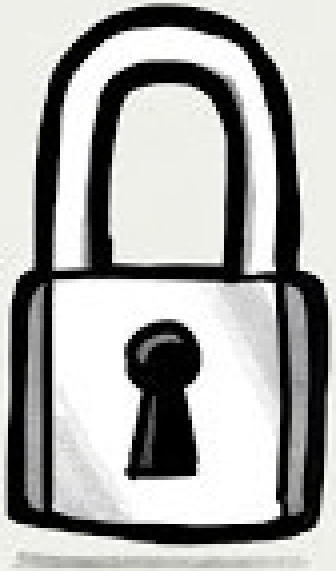
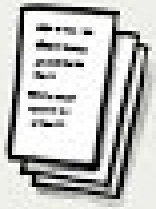
- Lernvideos
- Interaktive Quiz mit Fragen zu Cyber-Security Themen
- Firmeninterne Punktestände und Rangliste
- Checklisten, welche die wichtigsten Punkte anschaulich zusammenfassen



IT-Security Plattform
Das übersichtliche Cyber-Dashboard für den Geschäftsführenden. Dieses beinhaltet:

- Einen monatlichen IT-Sicherheitsbericht mit Handlungsempfehlungen, für eine erhöhte Sicherheit der IT-Systeme
- Aktuelle Information über Gefahren
- Zusammenfassung der Ergebnisse auf der Schulungsplattform






Massnahmen auf Kundenseite

Was muss das KMU weiterhin selbst erbringen?

Technische Massnahmen

- Virenschutz
- Firewall
- Backup (inkl. Testen)

Organisatorische Massnahmen

- Behebung der Schwächen aus dem IT-Infrastruktur-Scan
- Monitoring und Motivierung der Mitarbeiter anhand der Schulungsergebnissen
- Krisenübungen
- Business Impact Analyse über die maximal zu erwartenden Schäden

3

Zusammenfassung und Fragen

Vorteile AXA

Weshalb AXA der richtige Partner für Cyberversicherungen ist

10% Rabatt für Mitglieder des SVIT auf die Cyberversicherung
Gratisnutzung des Präventionsservice für einen Monat

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

Die **Soforthilfe** erfolgt für den Kunden **kostenlos**, auch wenn kein gedecktes Ereignis besteht

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

Das wichtigste nochmals auf einen Blick

AXA bietet mit dem Cyber Check & Schutz für KMU und dem Präventionsservice einen USP!

80% der KMU waren bereits von einem **Cyberangriff betroffen**

70% aller Schäden wurden durch **Mitarbeiter verursacht**

Weil es die 100%ige Sicherheit nicht gibt!

Präventionsservice

Cyberversicherung

Quelle: Clarity on Cyber, KPMG, 2018; Deloitte: Cyber Security Reporting 2019

- Fragen?
- Vielen Dank für Ihre Aufmerksamkeit

Für weitere Fragen wenden Sie sich an Ihren Versicherungsberater

AXA Versicherungen AG
Thomas Greub
Cyberversicherungen
General-Guisan-Strasse 40
8401 Winterthur
Telefon +41 58 215 26 84
thomas.greub@axa.ch
www.AXA.ch