Cyber Webinar WBG – Cyberrisiken, Deckungen, Services und Schadenfälle

Webinar WBG Schweiz

Thomas Greub, Senior Underwriter AXA, 28.05.2024

Agenda

60 Min.

1. Cyberrisiken	Weshalb kann jedes Unternehmen betroffen sein? Weshalb kann jede Wohnbaugenossenschaft betroffen sein? Umfragen, Statistiken Risiken der Immobilienbranche
2. Schadenfälle	
3. Angebote der AXA	Nutzen der Cyberversicherung Neuer Präventionsservice
4. Zusammenfassung und Fragen	


1
Cyberrisiken


Weshalb kann jedes Unternehmen
betroffen sein?

Zahlen

Quelle: Polizeiliche Kriminalstatistik 2023 / Bundesamt für Statistik (admin.ch)

- Seit erstmaliger Veröffentlichung 2020: jährlicher Anstieg der digitalen Kriminalität
- Im 2023: **43’839** gemeldete Straftaten mit digitalem Tatvorgehen
- **31.5%** Zunahme zum Vorjahr
- Grösster Anteil (40’469) **Cyber-Wirtschafskriminalität** (Wachstum von **36.5%**)
  - Phishing (+68.9%)
  - Missbrauch von Online-Zahlungssysteme (+66.1%)
  - Bezahlte aber nicht gelieferte Ware auf Kleinanzeigeplattformen (+23.1%)

- Nicht zu Wirtschaftskriminalität gehört: Cyber-Sexualdelikte und Cyber-Rufschädigung

Unternehmensziel: Informationssicherheit

Klären, was geschützt werden soll

Geistiges Eigentum
Wettbewerbsvorsprung

Datenschutz
Kundenvertrauen

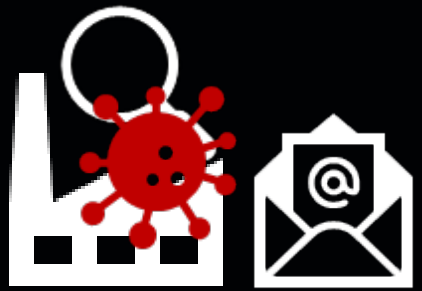
Rechtssicherheit
Haftung der Geschäftsführung

Schaden verhüten
Kosten reduzieren

Lieferfähigkeit
Verfügbarkeit der Waren

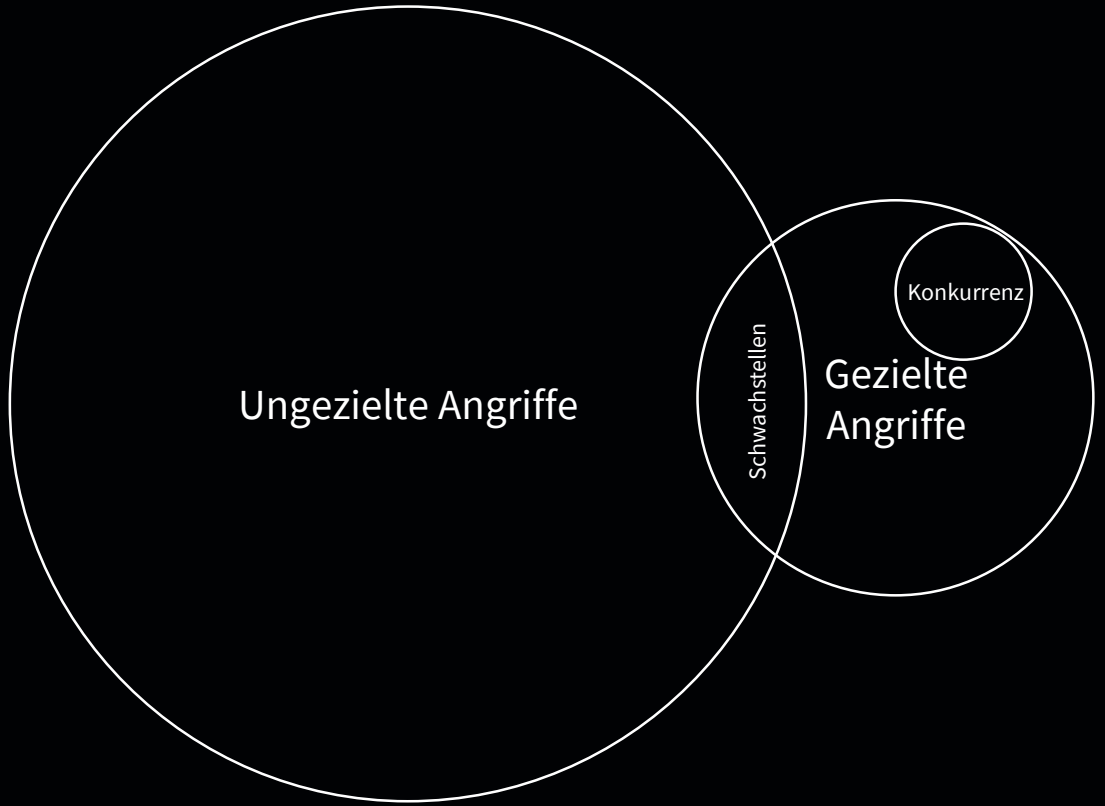
Festlegung
Risikoziele

Gezielte Angriffe



Ungezielte Angriffe

Ungezielte Angriffe



Täglich vernetzt

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 jede Wohnbaugenossenschaft betroffen sein?

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 und -käufen; 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)


1.3
Umfragen, Statistiken

“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

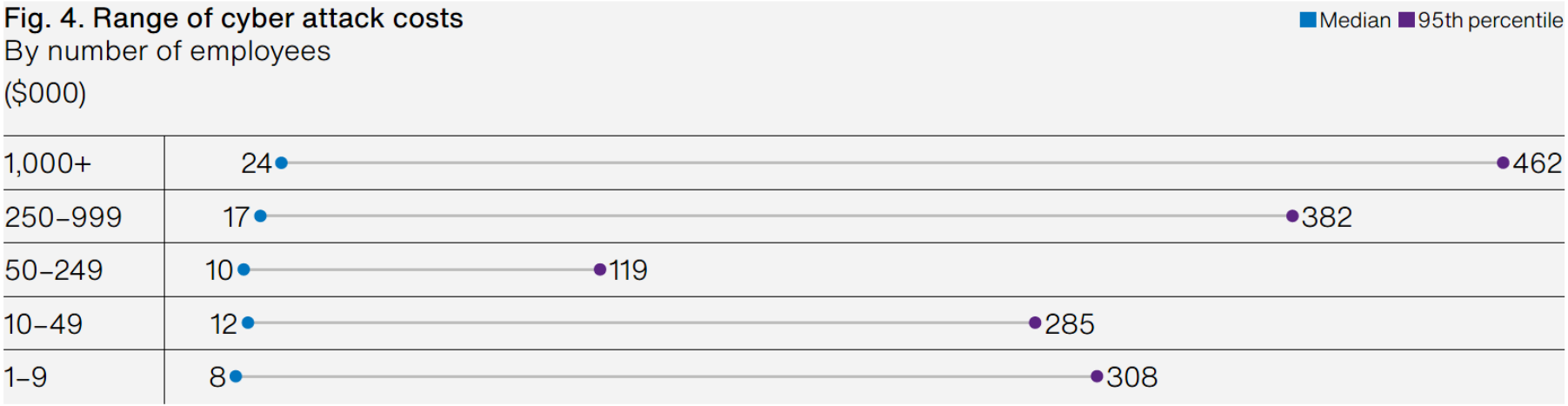
81%
unsere Computersysteme sind umfassend geschützt

58%
wir waren noch nie Opfer einer Cyberattacke

70%
unsere Daten sind nicht interessant

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

Welche Schadenhöhen sind zu verzeichnen?



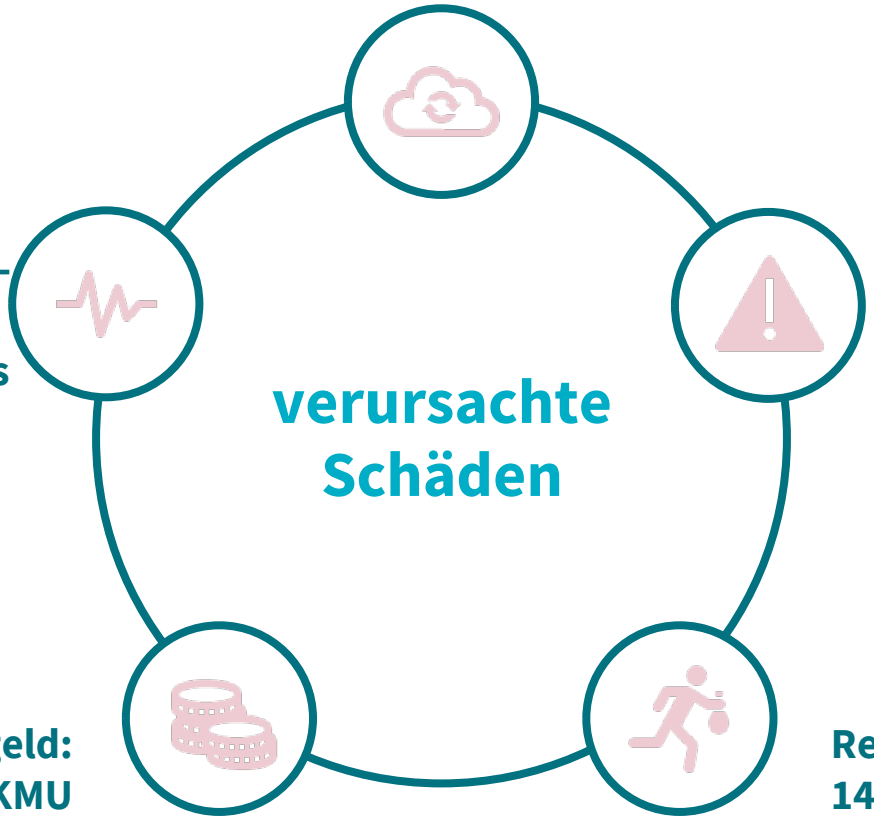
- Median bedeutet, dass 50% kleiner und 50% grösser sind als der Messwert.
- 95%-Perzentil bedeutet, dass 95% kleiner oder gleich gross sind wie der Messwert.

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**



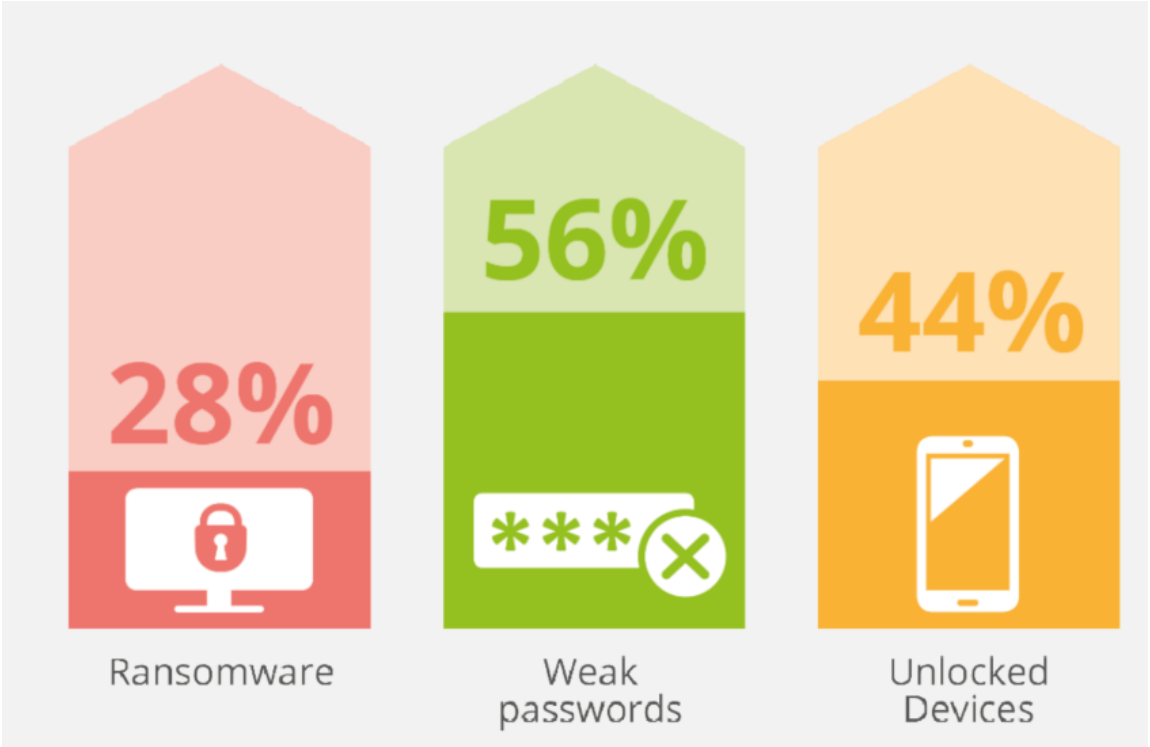
Diebstahl von Daten:
19% betroffene KMU

Zahlung von Lösegeld:
3% betroffene KMU

Reputationsschaden:
14% betroffene KMU

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

Wie dringen die Kriminellen ein?



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


2
Schadenfälle

Schadenfälle

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**

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


3
Angebote der AXA


3.1
Nutzen der Cyberversicherung

Cyberversicherung

Gefahr	Verdacht	Vorfall	Forderungen	Normalisierung
				
• Prävention • Finanzielle Sicherheit	• Incident Response/ Sofortmassnahmen	• Incident Response/ Sofortmassnahmen • Krisenmanagement • Notfallplan	• Datenschutz • Haftpflichtdeckung • Social Engineering • eBanking • Lösegeldforderung	• Wiederherstellung • Betriebsunterbruch • eBanking • Social Engineering • Telefonhacking

Produktübersicht Cyberversicherung

Grunddeckung

Eigenschäden
(inkl. Betriebsunterbruch)

Eigene Daten auf eigener IT
oder in einem Cloud-System

Haftpflichtschäden

Daten von Dritten

Krisenmanagement

Sofortmassnahmen, Kosten für
Krisenberatung
und –kommunikation

Zusatzdeckungen

Online Banking

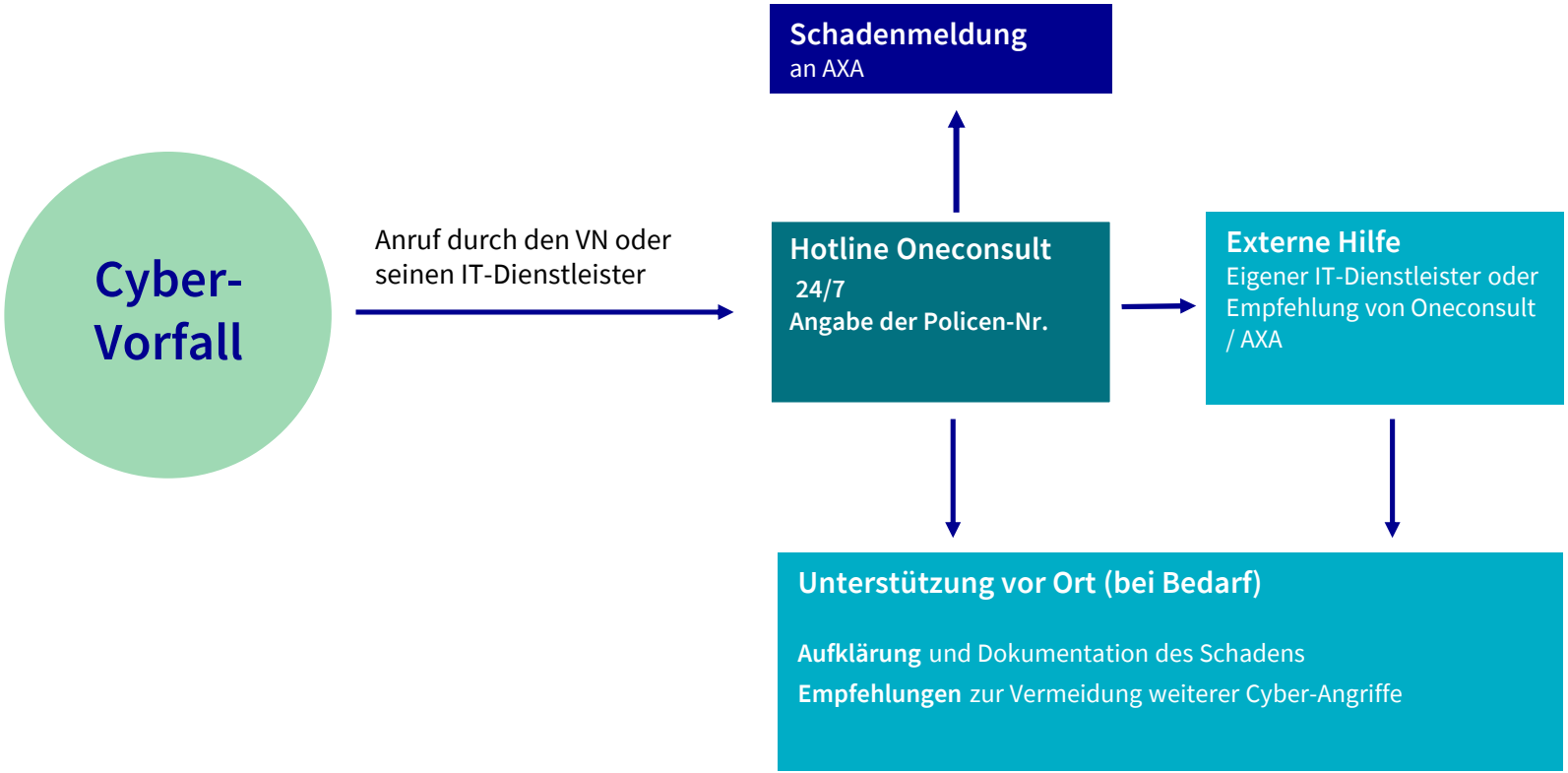
Social Engineering

Telefon Hacking

Zahlungen Lösegeld

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**

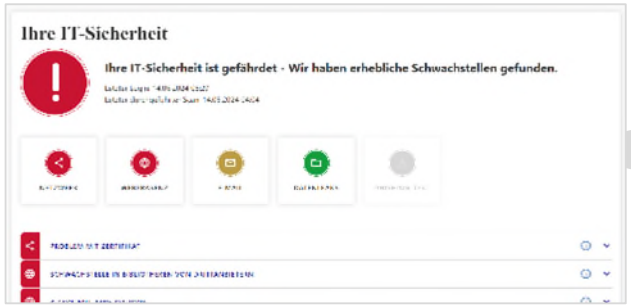
Obliegenheiten prüfen

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

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

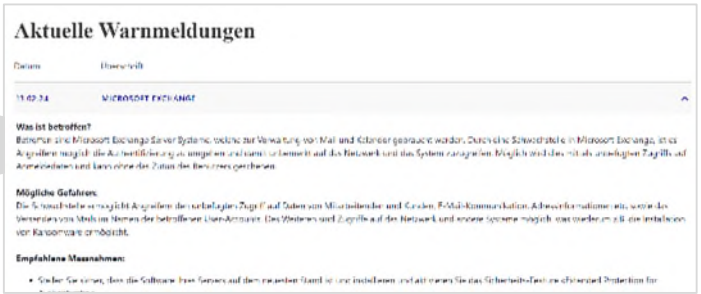

3.2
Neuer Präventionsservice
(seit 01.05.2024)

Neuer Präventionsservice - Inhalte



Überwachung von Schwachstellen im…
…Netzwerk
…Webseite
…E-Mail-Konfiguration
Überprüfung von **Datenleaks**

Warnmeldung für aktuelle **Schwachstellen**
Monitoring von Kreditkarten und Telefonnummern im Darknet



Phishing-Prävention mit Phishing Kampagnen an Mitarbeiter


4
Zusammenfassung und Fragen

Vorteile AXA

Weshalb AXA der richtige Partner für Cyberversicherungen ist

15% Rabatt für Mitglieder der WBG Schweiz auf die Cyberversicherung

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

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