Christian Parschik → Head of Digital Underwriting
Michael Vogl → Legal Claims Handler

# Effektiv gegen Cyber-Gefahren absichern mit einer Cyber-Versicherung

MARKEL

# Ihre heutigen Referenten

Christian Parschik

Head of Digital Underwriting

- → Seit April 2023 bei Markel
- → Seit mehr als 20 Jahren in der Versicherungsbranche
- → Verantwortlich für die Tarife auf den digitalen Plattformen & Tools
- → Berufliche Stationen: Allianz, Versicherungskammer Bayern, Finanzchef24, Münchener Verein

Michael Vogl

Legal Claims Handler

- → Seit November 2021 im Markel Claims-Team
- → Ansprechpartner für Cyber-Schäden und Koordination der Cyber-Dienstleister
- → 5-jährige Erfahrung als Rechtsanwalt im Bereich Versicherungsrecht und allgemeines Zivilrecht

# Agenda

1. Die Cyber-Gefahrenlage
2. Die Cyber-Gefahrenarten
3. Gefahr: Homeoffice (BYOD)
4. Prävention von Cyber-Attacken – Empfehlungen
5. Wie verhalte ich mich im Schadensfall?
6. Markel Pro Cyber – die moderne Art der Cyberversicherung

# Die Cyber-Gefahrenlage

01

# Cyber-Gefahrenlage auf einen Blick

**136.865**
registrierte Fälle von Cybercrime in 2022 *

**148,2 Mrd. €**
Schaden in der deutschen Wirtschaft durch Cyber-Attacken***

**25 %**
Anstieg Ransomware-Angriffe in 2. Jahreshälfte 2022 im Vergleich zum Vorjahr **

**18 %**
Der befragten Unternehmen gaben an, bereits Opfer eines **erfolgreichen Angriffs** gewesen zu sein **

**4 von 5**
Unternehmen haben IT Sicherheitslücken****

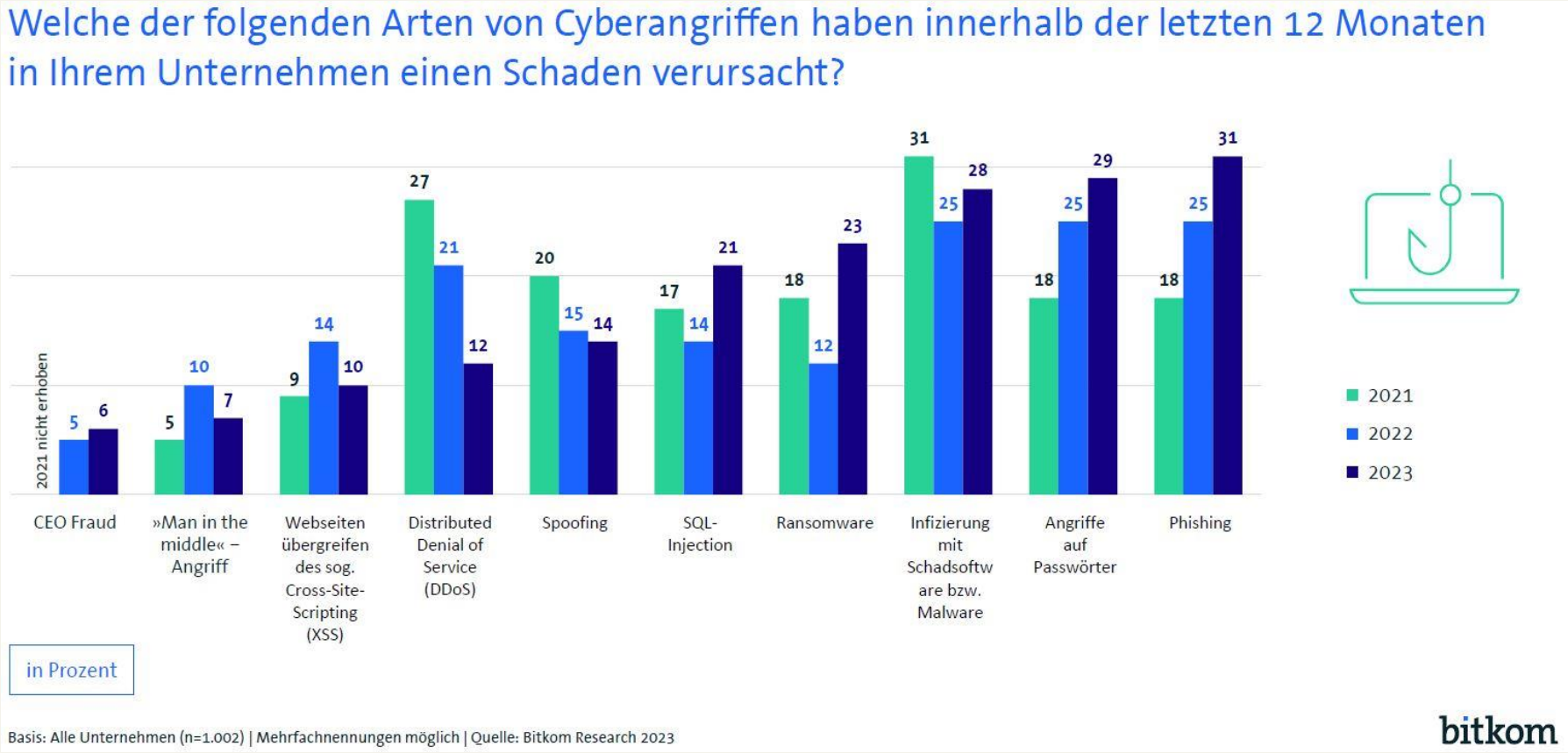
* BKA Bundeslagebild Cybercrime 2022

** TrueSec Threat Intelligence Report 2023

*** Bitkom Research 2023

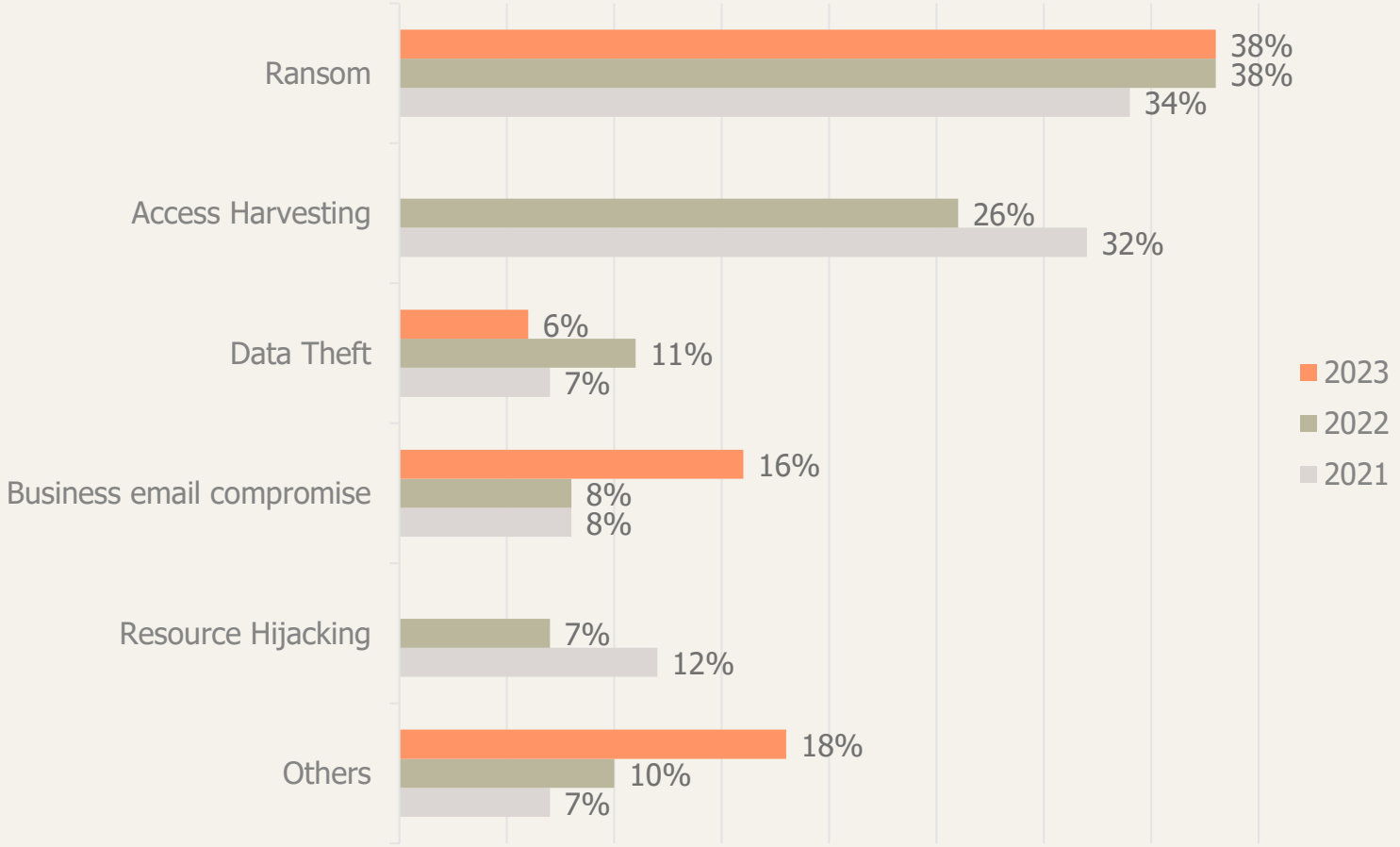
**** Repäsentative Forsa-Umfrage unter 300 Entscheidern kleiner und mittlerer Unternehmen im Mai/Juni 2023 (gem. Anhand Basis-Schutzmaßnahmen nach GDV-Bedingungen

# Arten von Cyberangriffen und deren Häufigkeit – Was sehen Führungskräfte?




Quelle: **Bitkom Research 2023** (Befragung von Führungskräften aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder Finanzen im Zeitraum KW16 bis KW 23 2023)

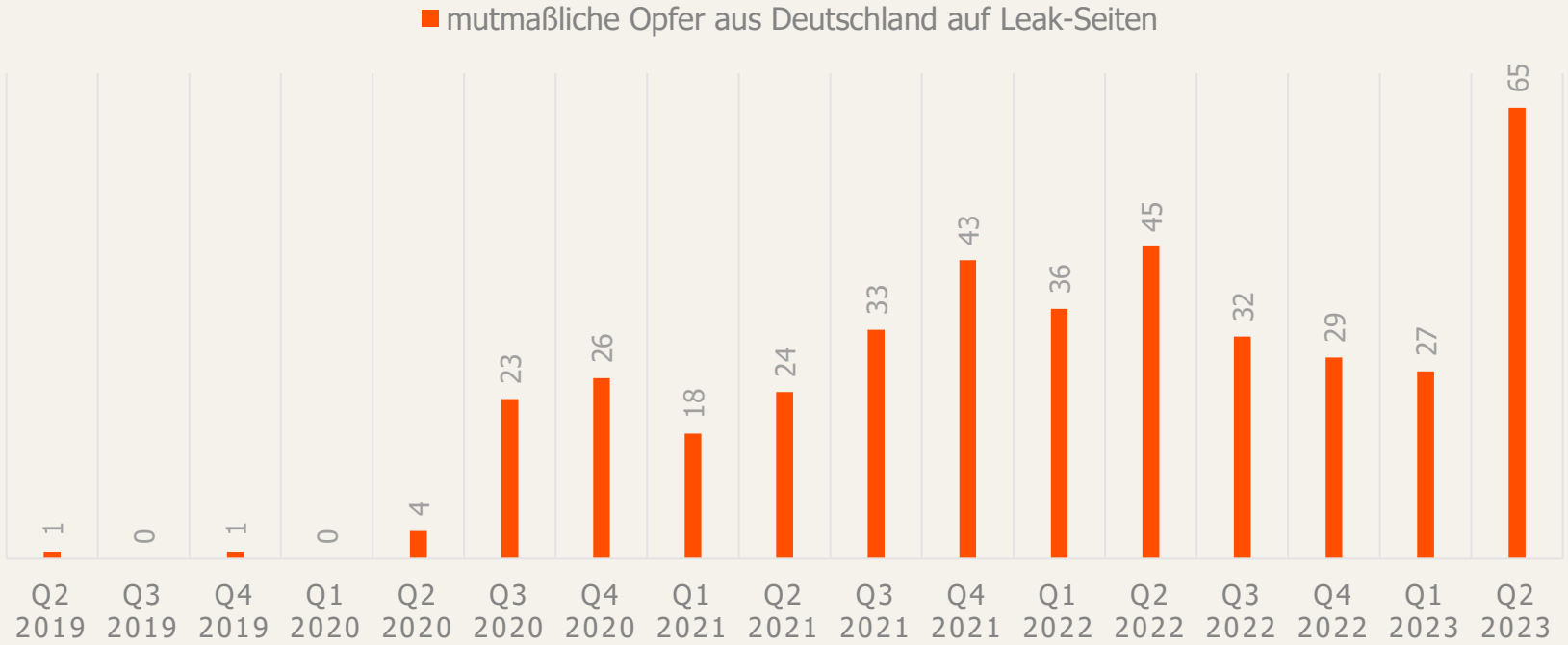
# Arten von Cyberangriffen und deren Häufigkeit – Was sagen Cyber-Experten?




Quelle: **TrueSec Threat Intelligence Report 2024**

Angaben in Prozent

# Double Extortion – mutmaßliche Opfer aus Deutschland auf Leak-Seiten




Quelle: **BSI – Die Lage der IT-Sicherheit in Deutschland 2023** (Leak-Opfer-Statistik des BSI)

- Ransom-Gruppen verstärken ihre Lösegeld-Forderung mit der Drohung sensible Unternehmensdaten zu veröffentlichen oder zu verkaufen
- Ransom-Verhandlungen werden zum Teil durch begleitende DDoS-Angriffe „unterstützt"

# Supply-Chain-Attack

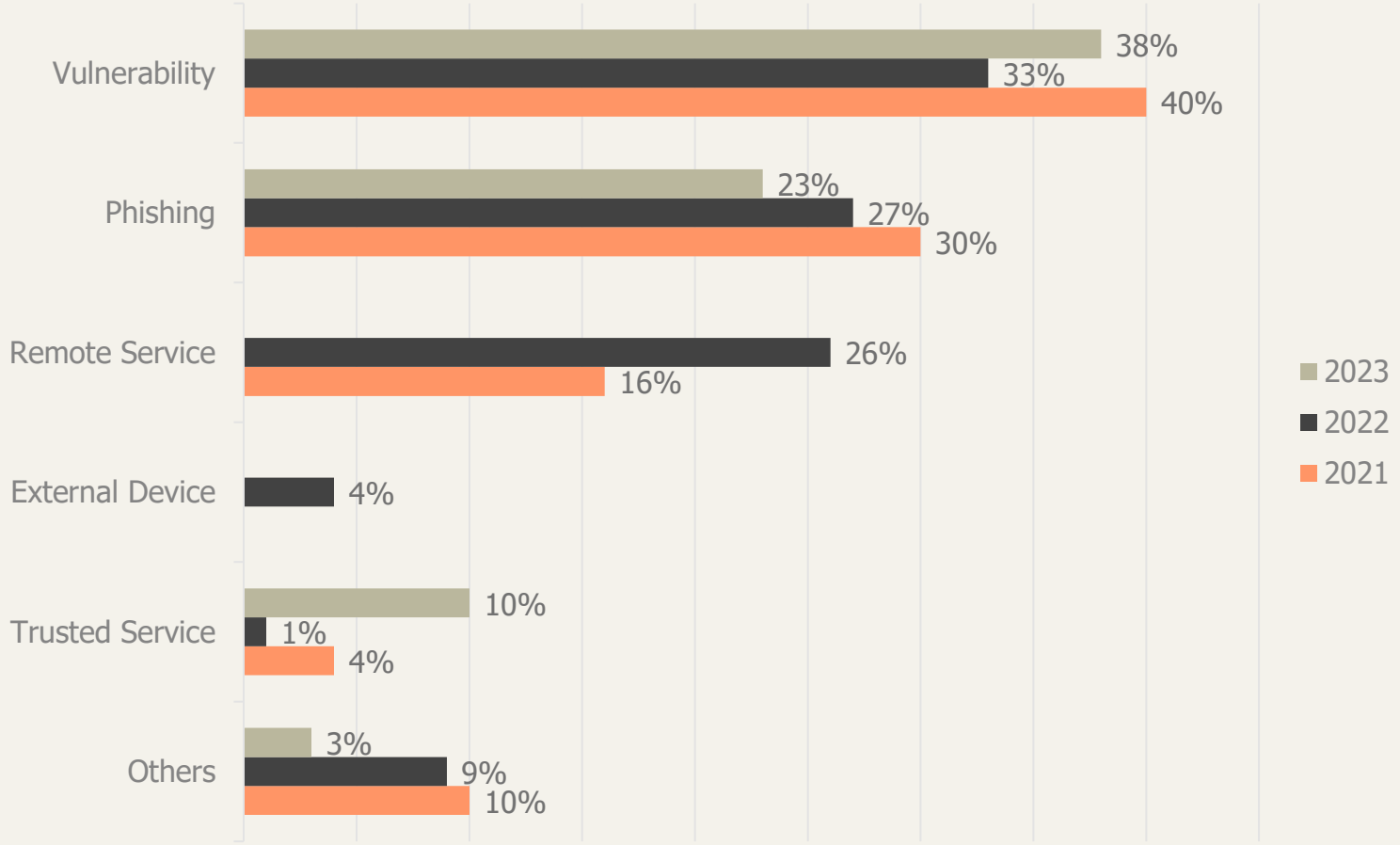
Cyber-Kriminelle | SaaS-Anbieter | Kunden

- Cyber-Kriminelle attackieren SaaS (Software-as-a-Service)-Anbieter
- Dessen Kunden können bereitgestellte cloud-basierte Dienste nicht mehr nutzen
- Kunden können nicht oder nur teilweise arbeiten → möglicherweise Betriebsunterbrechung
- Saas-Anbieter sieht sich Schadensersatzansprüchen von Kunden ausgesetzt

# Cyber-Gefahrenarten

02

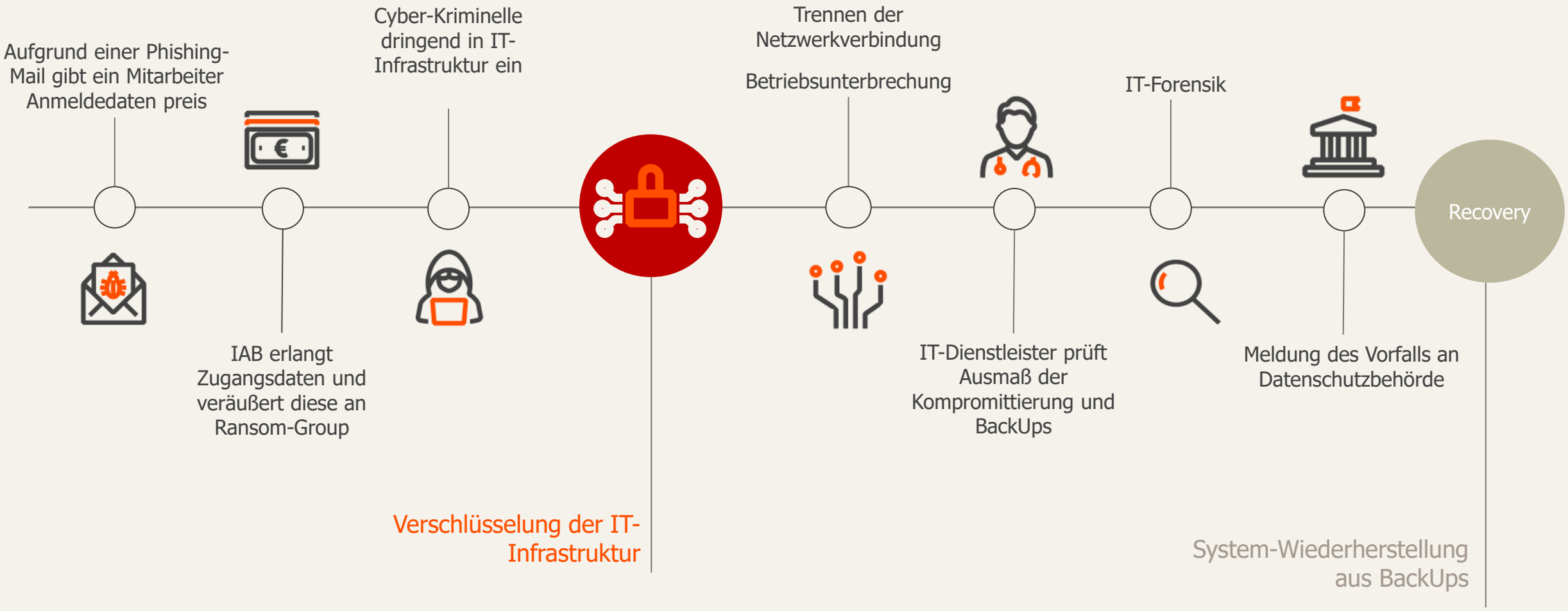
# Angriffsvektoren / Einfallstore




Quelle: **TrueSec Threat Intelligence Report 2024**

Angaben in Prozent

# (möglicher) Ablauf eines Ransomware-Angriffs



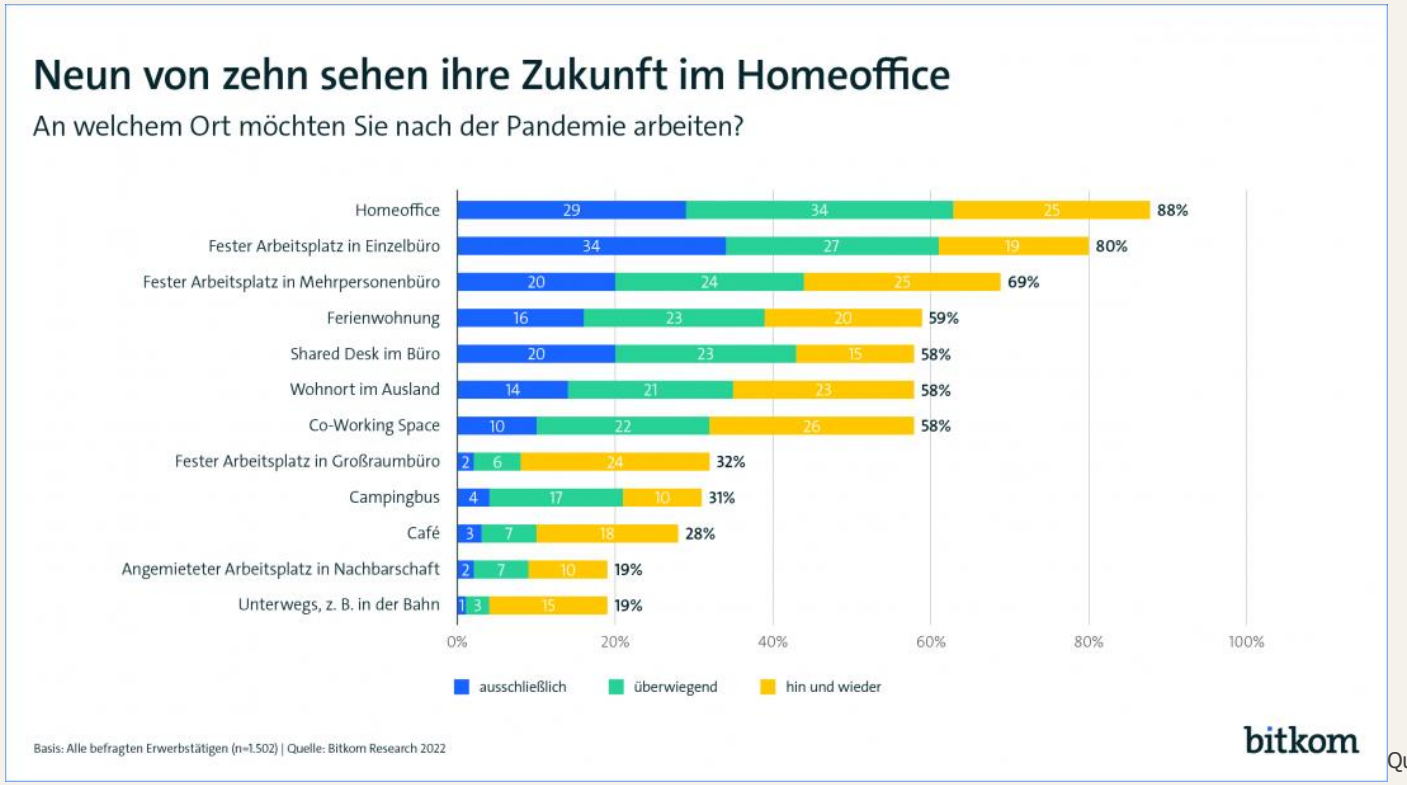
# Gefahr: Homeoffice (BYOD)

03

# IT-Sicherheit im Homeoffice

## New Work – Die Hälfte der Deutschen arbeitet im Homeoffice

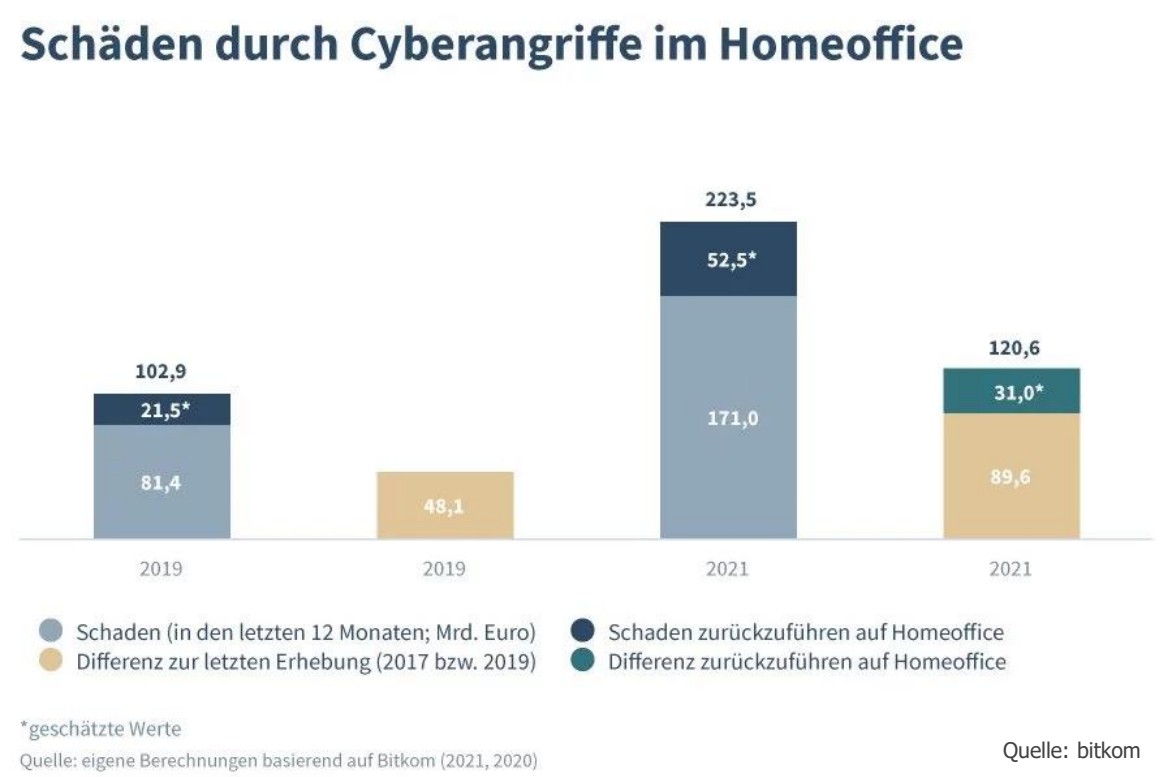
Corona hat die Arbeitswelt verändert und Homeoffice wurde zum festen Bestandteil.




Quelle: bitkom

Was bedeutet das für die Cyber-Sicherheit im Unternehmen?

# In Zeiten von Corona stiegen die Angriffe im Homeoffice stark an




Quelle: bitkom

Der Anstieg der Schäden durch Cyberangriffe im Homeoffice während der Pandemie im Vergleich zu 2019, der Corona-Homeoffice-Effekt, beträgt dementsprechend 31 Mrd. Euro oder 25,70 Prozent des Gesamtschadenanstiegs.

# Was sind die Probleme im Homeoffice?

**Firmengerät**

- kostenintensiv
- hoher Aufwand für IT-Admins
- Firmengelände ist besser gesichert
- direkter Kontakt zu Mitarbeitern

**Privatgerät**
**(BYOD – „Bring-Your-Own-Device“)**

- kostengünstig für AG
- IT-Admins haben keinen Zugriff
- wichtige Sicherheitsupdates werden oft nicht installiert
- Gefahr von veralteten Betriebssystemen
- Trennung zwischen privat und beruflich kaum möglich
- Homeoffice, freier Zugang für Familie, Freunde, Bekannte
- privates W-LAN wird von anderen Personen genutzt, entspricht oftmals nicht den Firmen Sicherheitsstandards
- digitaler Kontakt zu Kollegen (Phishing, Deep Fakes)

# Nutzung und Vorteile - Homeoffice

13% **Erfassung von…** Arbeitszeit, Spesen und ähnlichen Geschäftsfunktionen

21% **Verbinden sich mit Sozialen Netzwerken**

30% **Lesen und Schreiben**

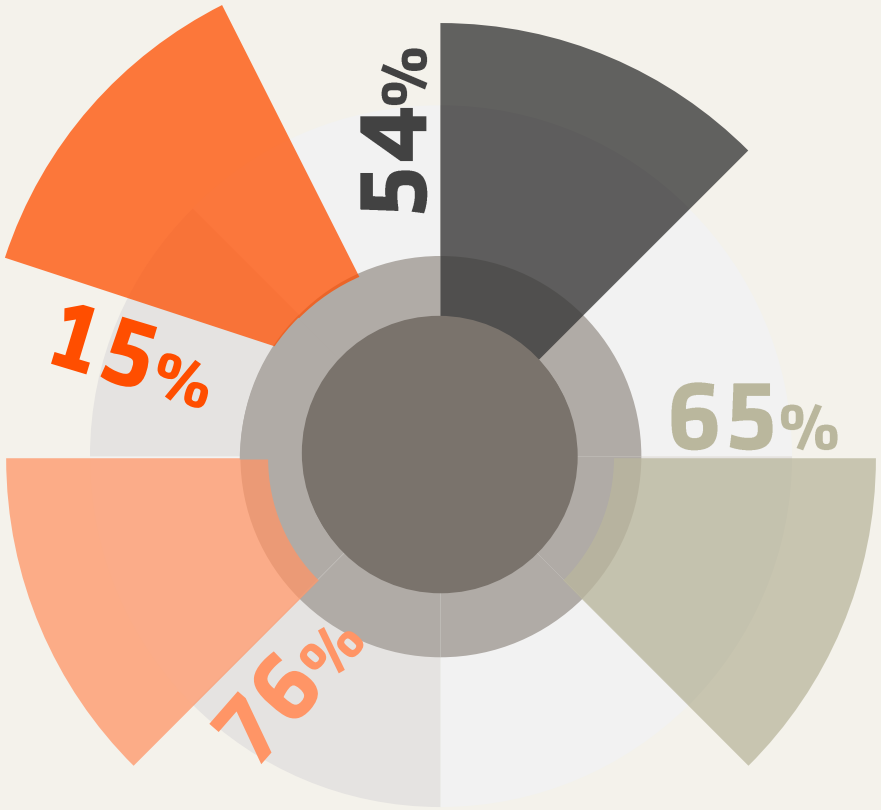
41% **Greifen auf E-Mails zu**

71% **Arbeiten auf einem vertrauten Gerät**

58% **Erhöhte Produktivität**

55% **Kostenersparnis**

# Bring your own device – Die Risiken




Von den **70 MILLIONEN** Geräten, die jedes Jahr verloren gehen oder gestohlen wurden, werden
**NUR 7%** wieder gefunden

## Daten

**15%** der Angestellten haben Zugriff auf sensible Daten via nicht zugelassener Geräte

## Encryption

**76%** der Unternehmen nutzen keine verschlüsselten Geräte

## Backup

**54%** der Unternehmen inkludieren private Geräte nicht in ihr Backup

## Löschen

**65%** der Unternehmen können Geräte nicht per Remote zurücksetzen

# Bring your own device – Die sichere Nutzung

- Kennwörter sollten auf allen BYOD-Geräten obligatorisch sein
- Setzen Sie etwaige Anwendungen auf eine schwarze Liste
- Beschränken Sie den Zugang zu Daten
- Investieren Sie in zuverlässige Sicherheitslösungen für Geräte
- Sichern Sie Ihre Daten auf Geräten regelmäßig
- Schulen Sie Ihre Mitarbeiter zum Thema Sicherheit

# Prävention

04

# Wie kann ich mich vor Cyber-Angriffen schützen

## Benennen Sie einen Hauptverantwortlichen für die IT-Sicherheit!

- Bewusstsein bei der Unternehmensleitung schaffen
- Die Zuständigkeit für die Umsetzung von Maßnahmen festlegen

## Erfassen Sie ihre IT-Systeme!

- Auflistung aller verwendeten Komponenten
- Auflistung der eingesetzten Software
- Auflistung der Daten und der Datenverarbeitung
- Auflistung aller Zugriffsrechte
- Auflistung der IT-Verbindungen mit der Außenwelt

## Durchführung einer regelmäßigen Datensicherung! (Am besten täglich!)

- Identifizieren Sie die Daten, die gesichert werden sollen
- Legen Sie fest, wie häufig Datensicherung durchgeführt werden soll
- Wählen Sie ein geeignetes Speichermedium, mit dem die Daten gesichert werden soll
- Prüfen Sie, welche Daten verschlüsselt werden sollen

# Wie kann ich mich vor Cyber-Angriffen schützen

## Führen Sie Updates umgehend durch!

- Verwenden Sie aktuelle Hardware- und Softwarelösungen
- Aktivieren Sie automatische Updates
- Legen Sie fest, wer für den Update-Prozess zuständig ist

## Deaktivieren Sie Makros!

- Makros sind kleine Programme, die man beispielsweise in Word-, Excel-, PPT oder PDF-Dateien einbetten kann

## Benutzen Sie einen Virenscanner und eine Firewall!

- Installation auf allen Systemen!

## Legen Sie eine Richtlinie für sichere Passwörter fest!

- Multi-Faktor-Authentifizierung (MFA)
- Mindestanzahl von Zeichen festlegen

# Empfehlung Cyber-Sicherheit für KMU – Die Top 14 Fragen

# Verhalten im Schadenfall

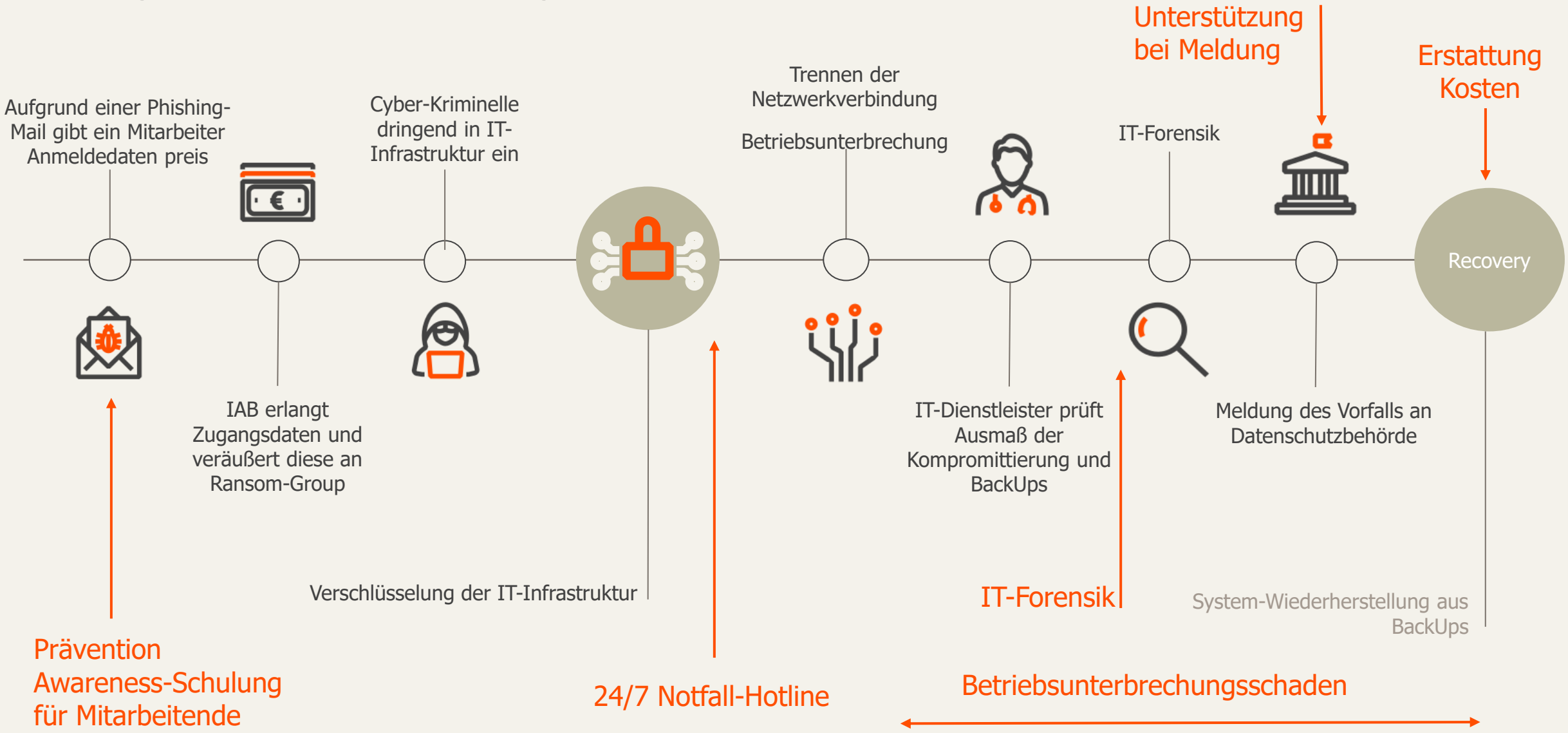
05

# Ransomware-Angriff

# Maßnahmen im Schadenfall

| | |
|---|---|
| Preparation | → Notfall-Plan<br>→ Mitarbeiter-Schulungen<br>→ Penetration-Test |
| Detection & Analysis | → Feststellen der Kompromittierung und möglicher Ursachen<br>→ ggfs. Unterstützung durch IT-Forensik<br>→ Welche Bereiche/Systeme sind betroffen? |
| Containment | → Betroffene Systeme vom Netz nehmen<br>→ Benutzer und Passwörter ändern |
| Eradication | → Malware oder ähnlich entfernen<br>→ BackUps checken<br>→ System überwachen |
| Recovery | → Je nach Ausmaß des Vorfalls ggfs. Systeme neu aufsetzen<br>→ (sichere) BackUps einspielen<br>→ Clients / Programme neu installieren |
| Post-Incident Activity | → Dokumentation<br>→ Auswertung des Vorfalls<br>→ Verbesserungen implementieren |

# Leistungen der Cyber-Versicherung im Schadenfall



# Markel PRO Cyber – Die moderne Cyber-Versicherung

06

# Welche Branchen versichern wir?

## Dienstleistung

- Arbeitsvermittlung
- Buchführungshelfer /-berater
- Immobilienmakler
- Reisebüro
- u.v.m.

## Freie Berufe

- Rechtsanwälte
- Steuerberater
- Wirtschaftsprüfer

## Handwerk- und Baugewerbe

- Baugewerbe
- Handwerk
- Logistik- und Transport

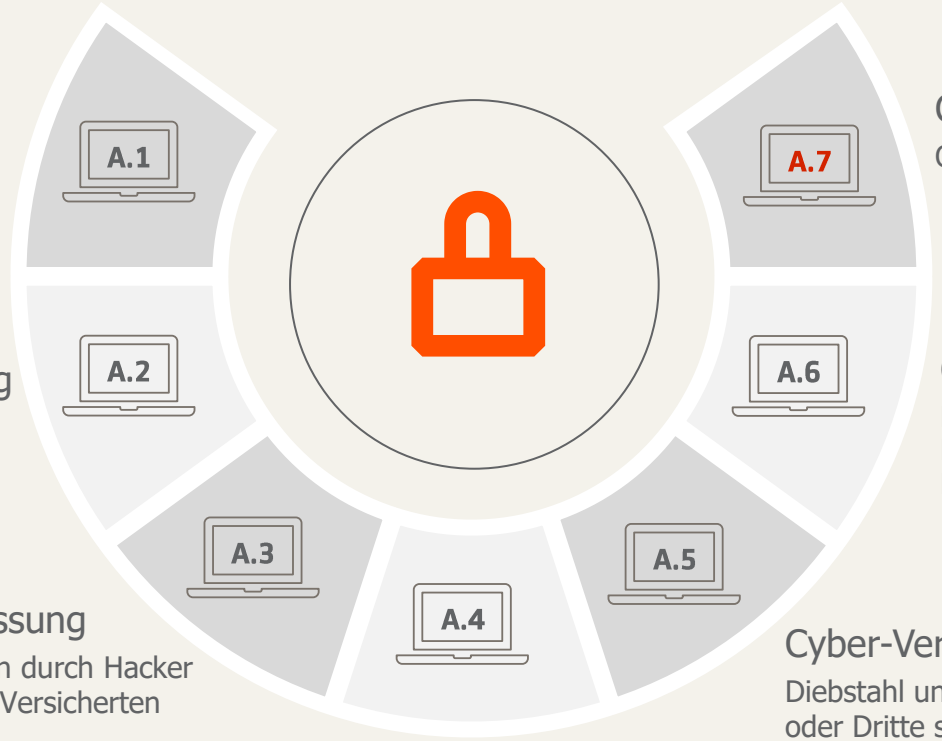
## Heilwesen

- Ärzte
- Pflegeeinrichtungen

## Vereine, Verbände und Bildung

- Sportvereine
- Interessensvereine
- Berufsverbände
- Schulen

# Modularer Versicherungsschutz




**Cyber Daten- und Eigenschäden**
Wiederherstellung der Hard- und Software

**Cyber Betriebsunterbrechung**
Ertragsausfall für den Zeitraum der versicherten Betriebsunterbrechung

**Cyber-Erpressung**
Geldforderungen durch Hacker gegenüber den Versicherten

**Cyber-Zahlungsmittel**
Forderungen der Kreditkartenindustrie wie z. B. Banken oder PayPal

**Cyber-Vertrauensschaden**
Diebstahl und Betrug durch mitversicherte Personen oder Dritte sowie Fake-President, Social-Engineering

**Cyber-Haftpflicht**
Haftpflichtansprüche seitens Dritten aus den Bereichen des Datenschutzes (EU-DSGVO, BDSG)

**Cyber-Prävention Premium**
Online-Präventionsplattform von Perseus

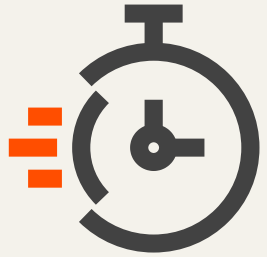
# A.1 Cyber Daten- und Eigenschäden – (Grunddeckung und Pflichtmodul)

Beinhaltet unter anderem →

- Sofort-Hilfe bei begründetem Verdacht (24h/7d)
- Wiederherstellung der IT-Systeme, Programme, Daten
- IT-Forensik
- Rechtsberatung zu gesetzlichen Pflichten des Datenschutzes
- Benachrichtigung der Betroffenen
- Public-Relations-/Reputations-Maßnahmen
- Sicherheitsanalyse und Sicherheitsverbesserungen
- Steuermehraufwendung

# A.2 Cyber-Betriebsunterbrechung

Keine Haftzeit !

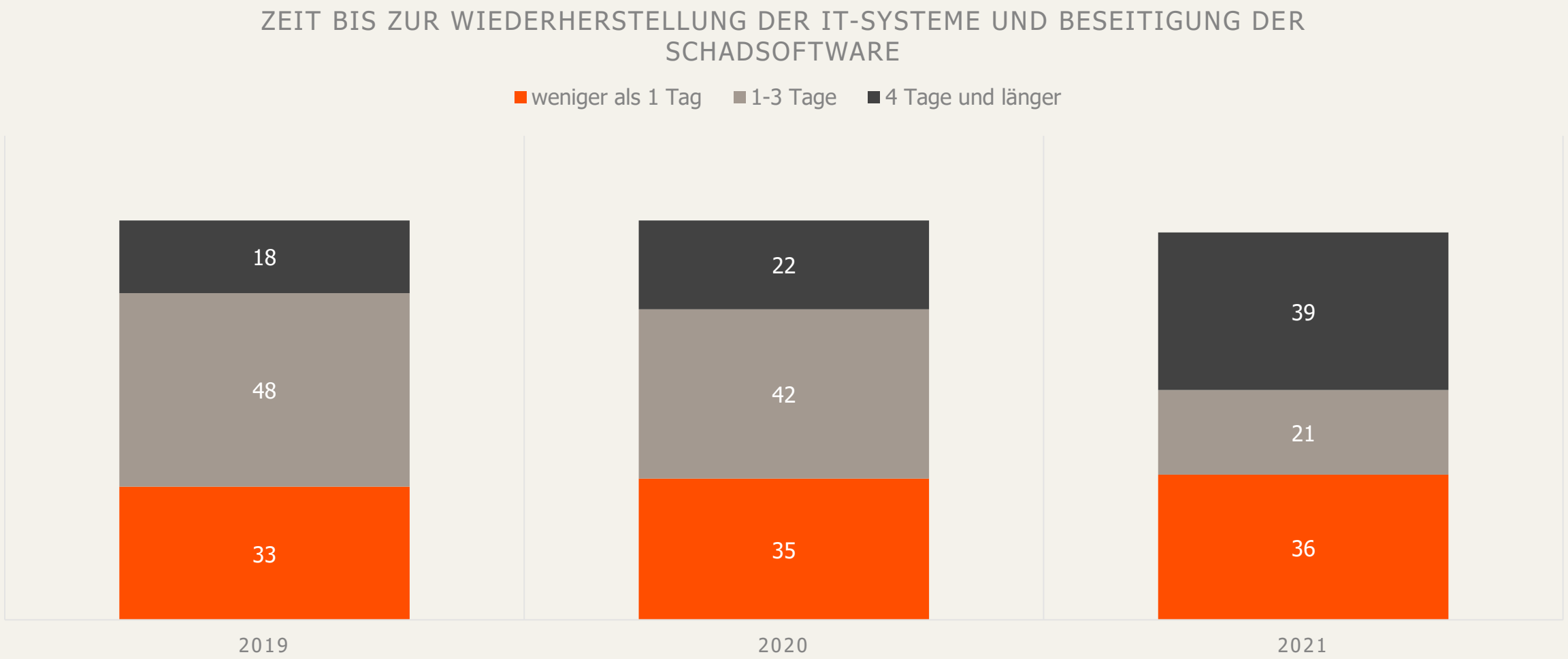


Beinhaltet unter anderem →

- Cyber-Betriebsunterbrechung bei Nutzung von Cloud- und Hosting-Diensten
- Cyber-Betriebsunterbrechung durch Verfügung einer Datenschutzbehörde
- Cyber-Betriebsunterbrechung infolge von technischen Problemen
- Vorleistung bei Nutzung von Cloud- und Hosting-Diensten

Es gilt ein zeitlicher Selbstbehalt von 8 Stunden, mindestens jedoch der gewählte Selbstbehalt des Hauptvertrags.

# Dauer der Betriebsunterbrechung – längere Ausfallzeiten



# A.3 Cyber-Erpressung

Beinhaltet unter anderem →

- Den Ersatz des gezahlten Geldbetrages
- Den Ersatz der Ware oder Dienstleistung
- Belohnungsgelder

# A.4 Cyber-Zahlungsmittel

## Versicherungsschutz bei dem Verstoß gegen

- Vertragspflichten von Kreditkartenverarbeitungsvereinbarungen mit einem Kreditinstitut,

- Anderweitige Vereinbarungen im Zusammenhang mit anderen Bezahlsystemen wie beispielsweise Bankkarten (EC-Karten),

- Vereinbarungen mit Zahlungsprozessoren und E-Payment-Providern, die den Schutz personenbezogener Daten im Sinne des § 3 Absatz 1 BDSG oder vergleichbarer ausländischer Rechtsnormen bezwecken, infolge eines Cyber- und Daten-Eigenschadens.

# A.5 Cyber-Vertrauensschaden

## Vertrauensschäden durch eigene Mitarbeiter

- Betrug
- Urkundenfälschung
- Unterschlagung
- Diebstahl von Firmengeldern, Kundendaten, Waren, etc.

## Vertrauensschäden durch Dritte

- Betrug
- Urkundenfälschung
- Unterschlagung
- Diebstahl von Firmengeldern ( z.B. Phishing von Bankdaten), Kundendaten, Waren, etc.

Fake President und andere Social Engineering Schäden gelten auch als versichert!

# A.6 Cyber-Haftpflicht

- Verstöße gegen die Cyber-Sicherheit (Weitergabe von Schadsoftware)
- Verstöße gegen den Datenschutz
- Verstöße gegen Geheimhaltungspflichten
- Vertragsstrafen bei Verletzung von Geheimhaltungspflichten
- Verstöße gegen Namens- und Persönlichkeitsrechte
- Verstöße durch Werbung und Marketing
- Straf- oder Bußgelder gelten mitversichert (sofern gesetzlich erlaubt)
- Freistellung externer Datenverarbeiter
- Straf- und Ordnungswidrigkeitenrechtschutz

# A.7 Cyber-Prävention

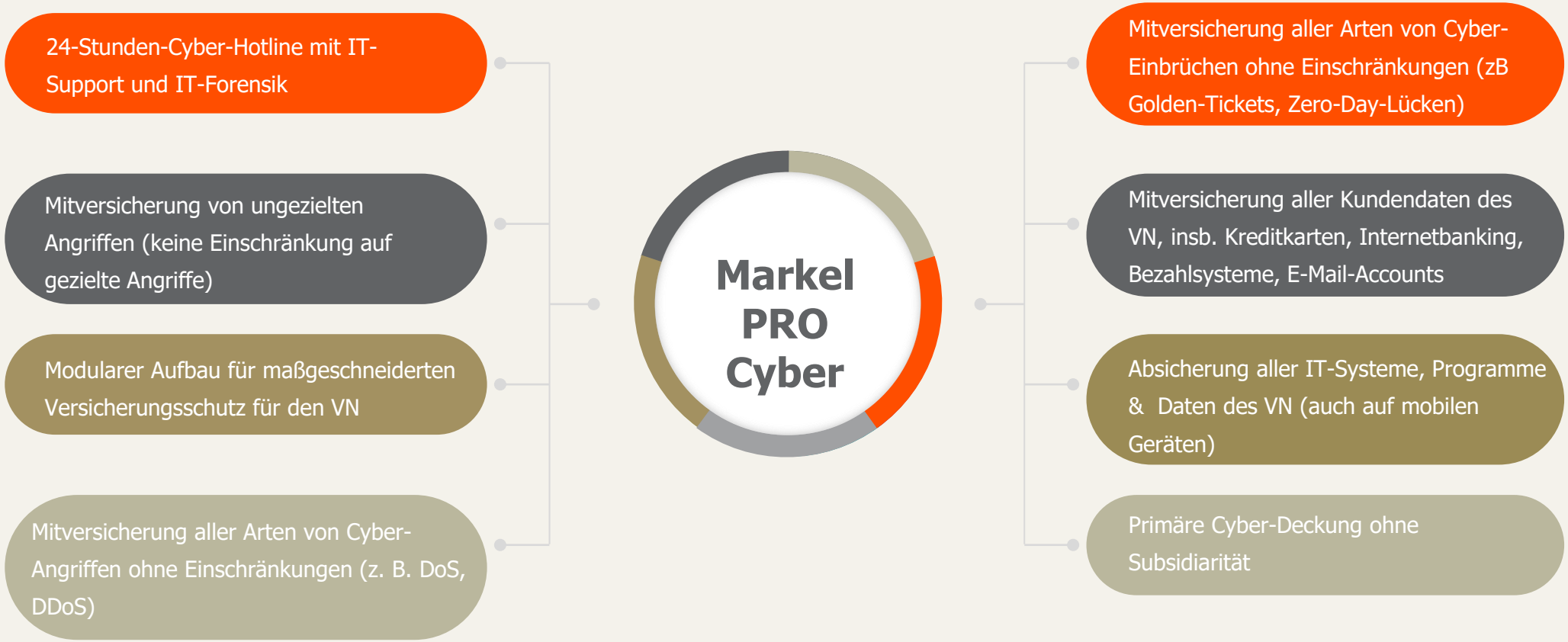
## Cyber-Prävention Basis (prämienneutral enthalten)

- ✓ Einmalige IT-Sicherheitsprüfung
- ✓ Online-Training Cybersicherheit & Datenschutz für maximal 3 Mitarbeiter
- ✓ Einmaliger Phishing-Test
- ✓ Browser-Check, Passwort Erinnerung
- ✓ Blog, Newsletter & Glossar

## Cyber-Prävention Premium

- ✓ Online-Training für Cybersicherheit und Datenschutz für unbegrenzte Anzahl von Mitarbeitern & Zertifikate
- ✓ Laufende Phishing-Tests
- ✓ Sicherheitsassistent für Admins
- ✓ Darknet-Scan, Browser-Check, Passwort Erinnerung, E-Mail-Scanner
- ✓ Systematische und gezielte Aktivierung der Mitarbeiter zur Nutzung der Tools
- ✓ Gefahrenwarnungen
- ✓ Reporting Bereich mit Online-Trainings-Statistik und Cyber-Sicherheits-Scores

# Markel Pro Cyber - Highlights

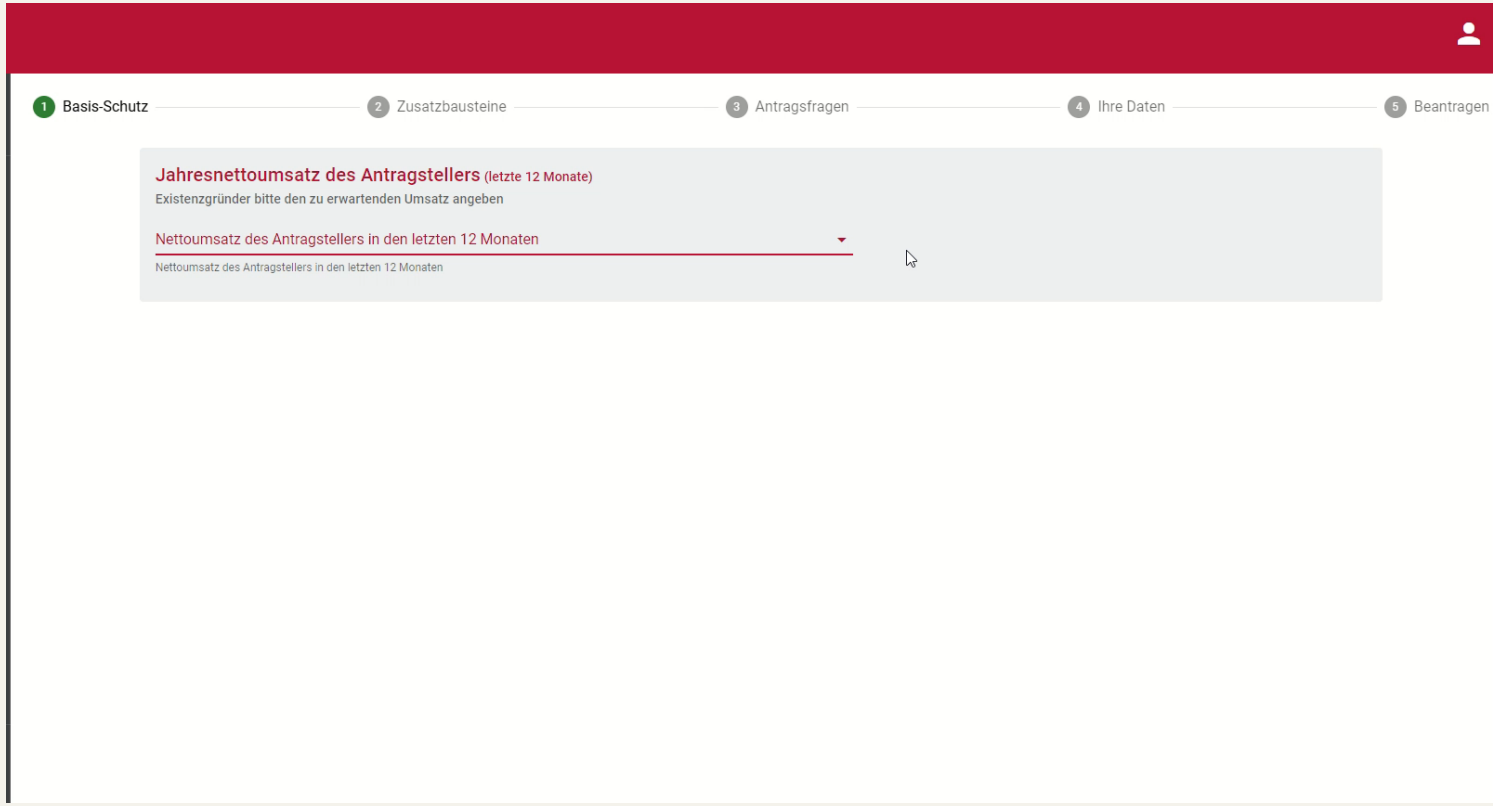


# MarkelNow

**Das neue exklusive Maklerportal für den modernen Makler.**

→ Direkt online beantragen
→ Policen ohne Wartezeit
→ 24/7 – rund um die Uhr
→ Einfach und intuitiv
→ Service für Ihre Kunden optimieren
→ Kundenzufriedenheit steigern
→ Sicherer, DSGVO-konformer Zugang

**Hier kostenfrei Zugangsdaten beantragen:**
www.markel.de/markelnow



# Folgen Sie uns schon auf LinkedIn?

MARKEL

# Verwendete Quellen

| Quelle / Link | Jahr | Folienseite |
|---|---|---|
| **Bitkom Research 2023** (Befragung von Führungskräften aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder Finanzen im Zeitraum KW16 bis KW 23 2023) | 2023 | 5, 6 |
| **BKA** Bundeslagebild Cybercrime 2022 | 2023 | 5 |
| **BSI – Die Lage der IT-Sicherheit in Deutschland 2023** (Leak-Opfer-Statistik des BSI) | 2024 | 8 |
| **TrueSec** Threat Intelligence Report 2023 | 2024 | 5, 7, 11 |
| Repäsentative Forsa-Umfrage unter 300 Entscheidern kleiner und mittlerer Unternehmen im Mai/Juni 2023 (gem. Anhand Basis-Schutzmaßnahmen nach GDV-Bedingungen) | 2023 | 5 |
| **Bitkom Research 2022** | 2022 | 14, 15 |
| Mobiles Arbeiten: Ein umfassender Blick auf Vor- und Nachteile - Net-Base Magazin | 2023 | 17 |
| Bring Your Own Device: Private Endgeräte im Unternehmen nutzen (pcspezialist.de) | 2021 | 18 |