Michael Vogl → Senior Legal Claims Handler
Marvin Knorr → Junior Legal Claims Handler

Aktuelle Schadenssituation in der Cyberversicherung

MARKEL

Ihre heutigen Referenten

Michael Vogl

Senior 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

Marvin Knorr

Junior Legal Claims Handler

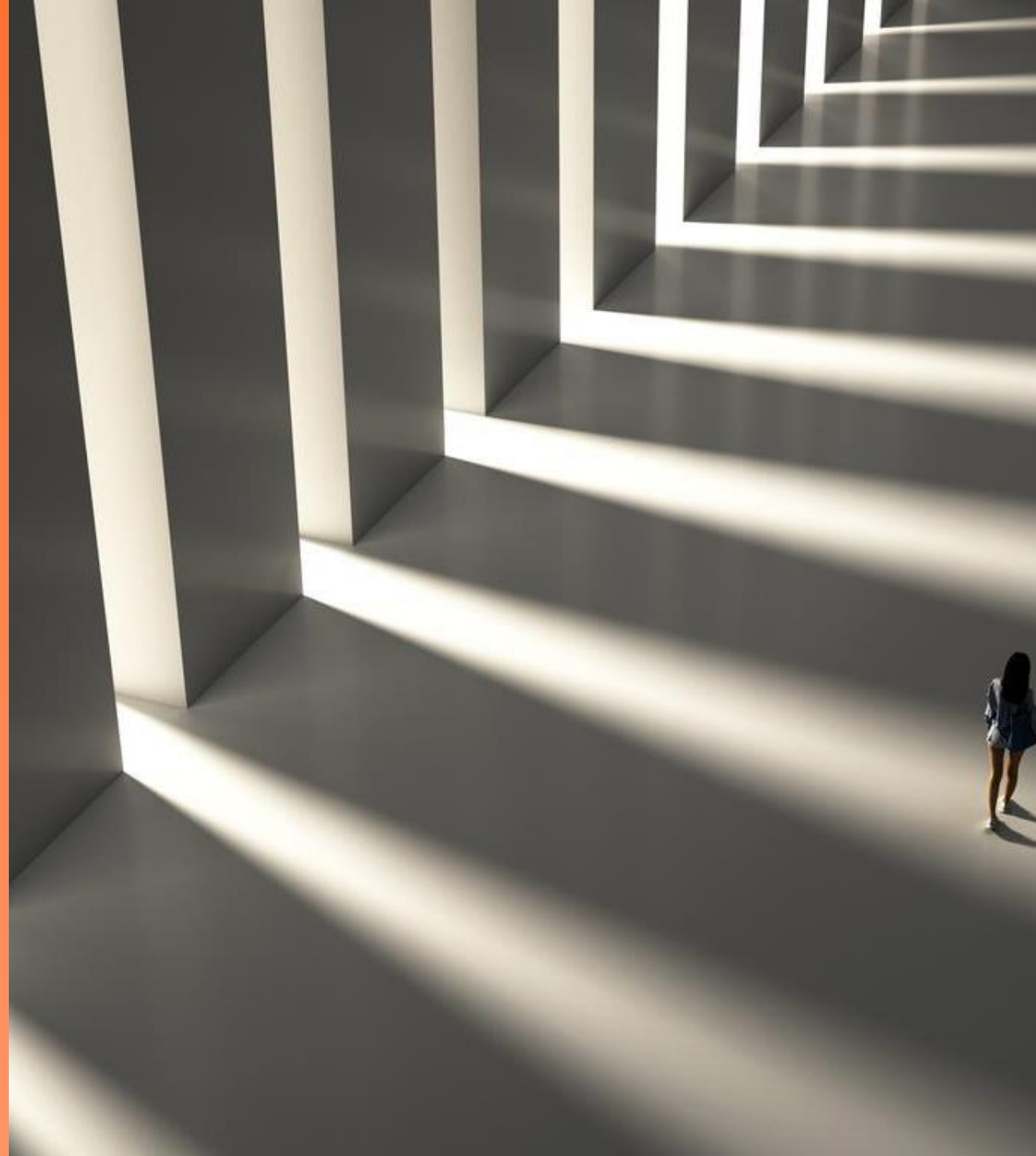
- → Seit September 2023 im Markel Claims-Team
- → Ansprechpartner für Cyber-Schäden
- → IT-Recht als Studienschwerpunkt

Agenda

1. Die Cyber-Gefahrenlage
2. Die Cyber-Gefahrenarten
3. Datenschutz und immaterieller Schadensersatz
4. Cyber-Vertrauensschäden
5. Verhalten im Schadenfall

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

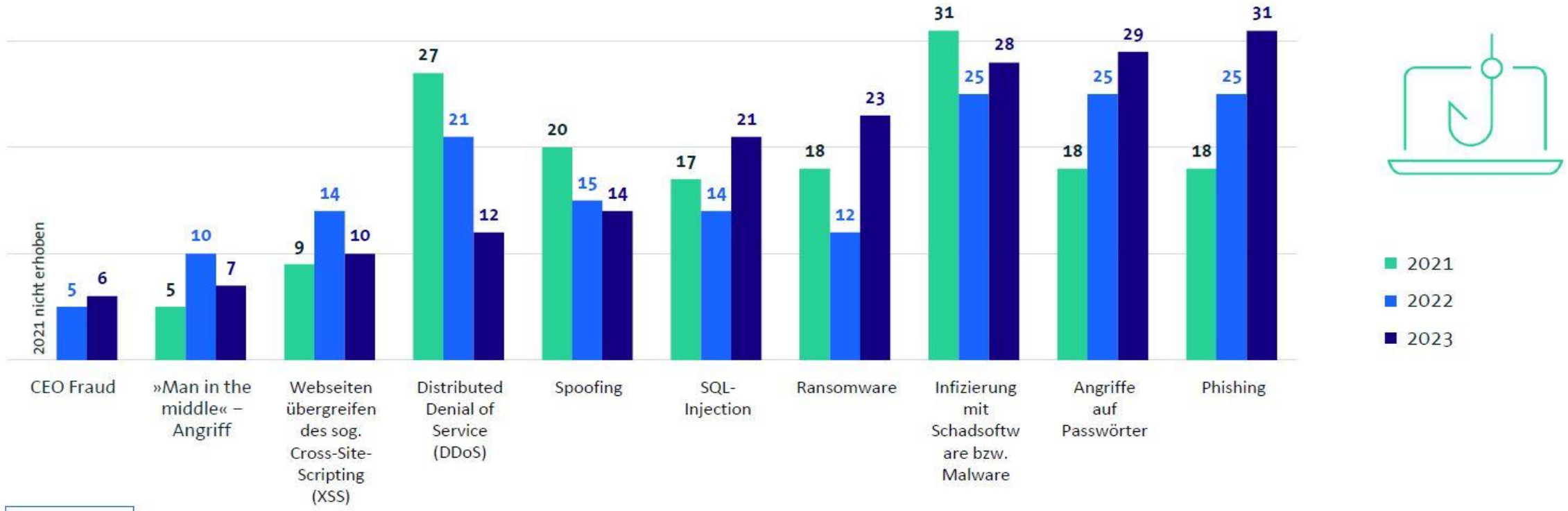
** TrueSec Threat Intelligence Report 2023

*** 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 – Befragung von Führungskräften

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?

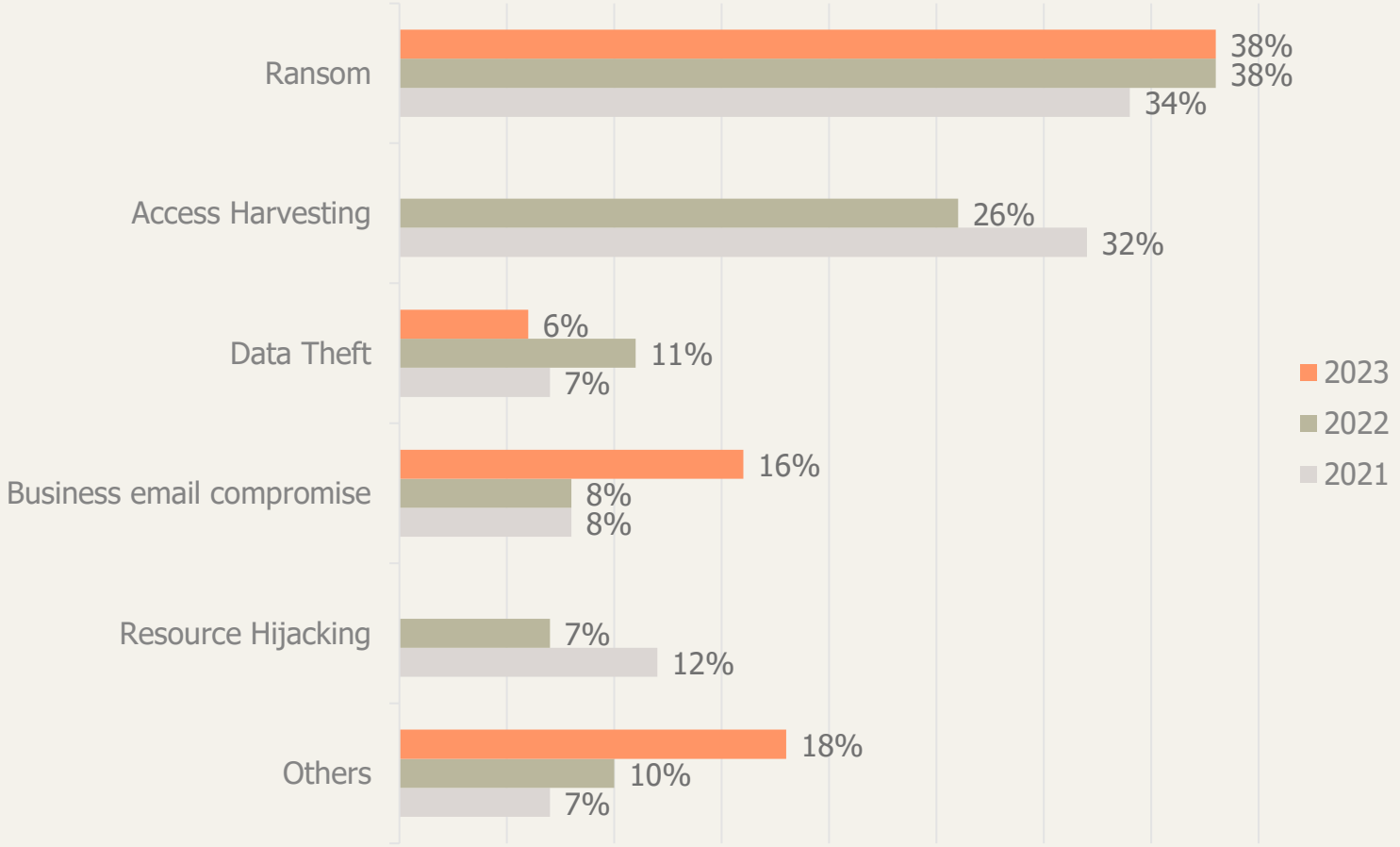


in Prozent

Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2023

bitkom

Arten von Cyberangriffen und deren Häufigkeit – Gemeldete Fälle bei Cyber-Experten



Quelle: **TrueSec Threat Intelligence Report 2024**

Angaben in Prozent

Supply-Chain-Attack

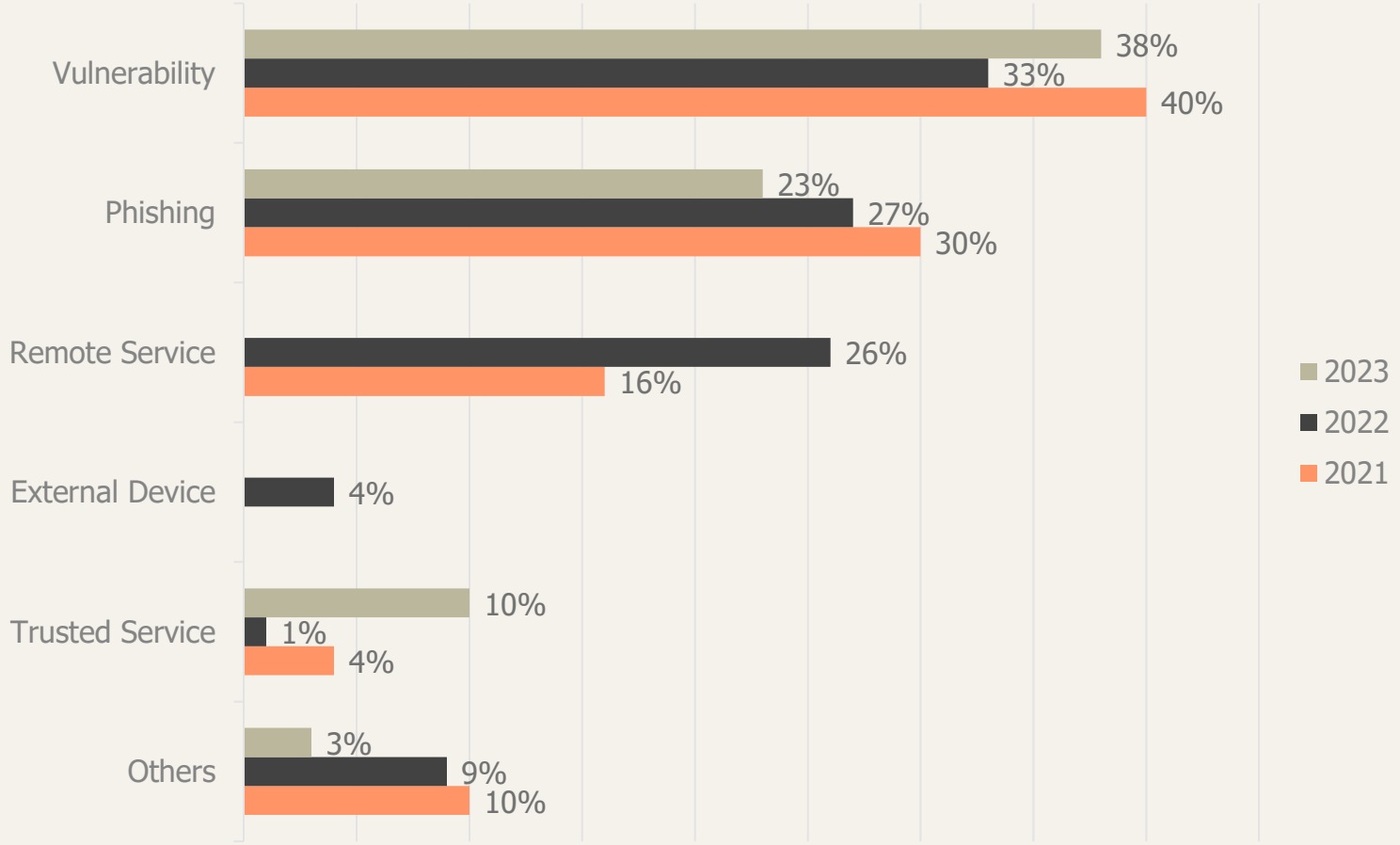
Cyber-Kriminelle | SaaS-Anbieter | Kunden

- 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

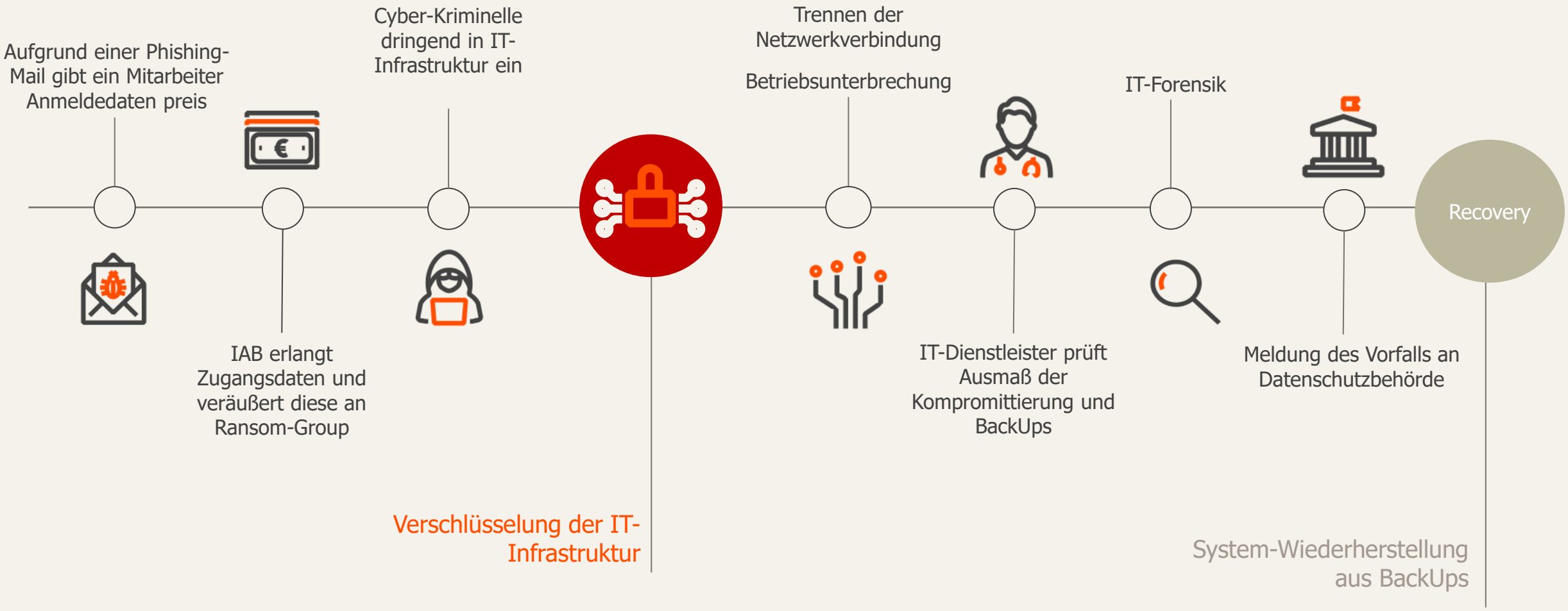
Angriffsvektoren / Einfallstore



Quelle: **TrueSec Threat Intelligence Report 2024**

Angaben in Prozent

(möglicher) Ablauf eines Ransomware-Angriffs



Datenschutz und immaterieller Schadensersatz

03

Schadenersatzpflicht der Verantwortlichen nach Art 82 DSGVO
EuGH v. 14.12.2023 (C-340/21)

Bei einem Cyber-Angriff auf eine bulgarische Behörde (Natsionalna agentsia za prihodite) sollen Hacker Zugriff auf personenbezogene Daten erlangt, und diese im Internet veröffentlicht haben. Betroffen waren mehr als 6 Mio natürliche Personen (sowohl bulgarische als auch ausländische Staatsbürger). Hierüber berichteten Medien ab 15.07.2019.

Einige hundert betroffene Personen erhoben Klage auf Ersatz des immateriellen Schadens, der sich aus der Offenlegung ihrer personenbezogenen Daten ergeben haben soll (Art. 82 DSGVO).

Instanz: Gericht weist Klage ab.
- Kläger haben nicht nachgewiesen, dass die Behörde es unterlassen hat, geeignete Sicherheitsmaßnahmen zu ergreifen

Entscheidung EuGH v. 14.12.2023 (C-340/21):

- Aus einem unbefugten Zugriff, kann nicht automatisch auf ein unzureichendes Schutz-Niveau geschlossen werden
- Aber: **Beweislast liegt beim Verantwortlichen**

- Immaterieller Schaden (gem. Art 82 GSGVO) bereits bei Befürchtung, personenbezogene könnten durch Dritte missbräuchlich verwendet werden.

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"

Cyber-Vertrauensschäden

04

Cyber-Vertrauensschäden

Beispiele

Man-in-the-middle

Ein Angreifer steht heimlich zwischen mehreren Kommunikationspartnern und fängt deren Kommunikation ab, manipuliert, oder steuert sie

Phishing

Angreifer verwenden betrügerische E-Mails, Websites oder andere Kommunikationsmethoden, um jemanden dazu zu bringen, sensible Informationen oder Daten freizugeben

Spoofing

Der Angreifer verschleiert seine Identität oder Herkunft, um sich als eine vertrauenswürdige Quelle auszugeben

Fake President

Angreifer gibt sich als hochrangiger Unternehmensführer aus, oft als GF, um Mitarbeiter dazu zu bringen, finanzielle Transaktionen durchzuführen

Cyber-Vertrauensschäden

Was ist passiert?

VN ist eine Steuerberatungsgesellschaft.

Am 25.09.2023 unterhielt sich die für Überweisungen zuständige Mitarbeiterin mit einer Geschäftsführerin der VN per E-Mail:

Von: Geschäftsführerin
Gesendet: Montag, 25. September 2023 10:35
An: Mitarbeiterin
Betreff: Zahlung

Wie hoch ist unser Kontostand? Können wir heute eine Auslandszahlung von 38.625,00 Euro machen? Es ist dringend.

Grüße,
Geschäftsführerin

Von: Mitarbeiterin
Gesendet: Montag, 25. September 2023 12:26
An: Geschäftsführerin
Betreff: AW: Zahlung

Hallo Geschäftsführerin

anbei unsere Kontostände Stand 22.09.2023 😉 Überweisungen ins EU-Ausland kann ich gerne machen, es gibt nur Probleme mit der Schweiz oder Drittländer.

Cyber-Vertrauensschäden

Was ist passiert?

Von: Geschäftsführerin
Gesendet: Montag, 25. September 2023 15:48
An: Mitarbeiterin
Betreff: AW: Zahlung

Ok. Bitte bearbeiten Sie diese Zahlung sofort. Hier sind die Zahlungsdaten:

KONTOBEZEICHNUNG:
ADDRESSE:
IBAN:
BIC:
SC:
KONTO NUMMER:
BANK:
ZWECK:
REFERENZ:

...Senden mir den Überweisungsbeleg.

Grüße,
Geschäftsführerin

Von: Mitarbeiterin
Gesendet: Dienstag, 26. September 2023 08:13
An: Geschäftsführerin
Betreff: AW: Zahlung

Guten Morgen Geschäftsführerin

anbei der Überweisungsbeleg 😉
Ich habe Ihre Mail gerade erst gelesen und gleich ausgeführt.

Viele Grüße
Mitarbeiterin

Es stellte sich heraus, dass es sich bei der angeblichen Geschäftsführerin um einen Betrüger handelt.

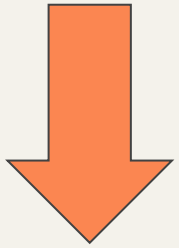
Noch am selben Tag wendet sich VN an die Cyber-Schaden-Hotline unseres externen IT-Spezialisten BeforeCrypt (BC). BC sendet uns einen Damage Report, der die wesentlichen Informationen zum Schadensfall enthält.

Cyber-Vertrauensschäden

Der Gang bei Markel

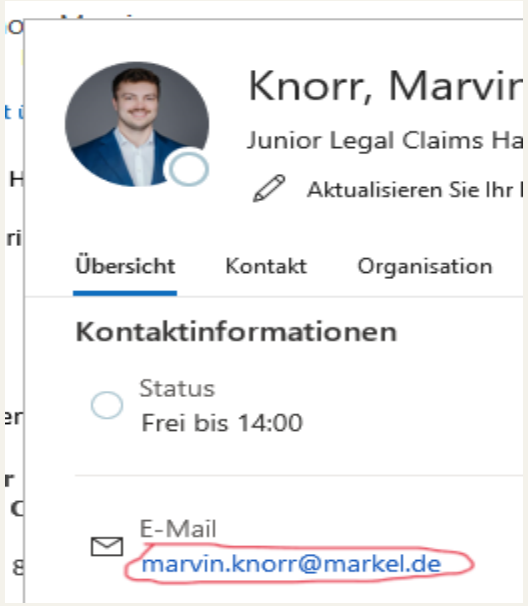
Erste (kurze) Deckungsprüfung: Besteht die Police, versicherter Zeitraum, versicherte Tätigkeit?

Während diesem Schritt prüfte BC bereits, ob sich der Betrüger möglicherweise Zugang zu den Systemen der VN verschafft hat. Zusätzlich musste geklärt werden, ob der Betrüger von außen oder aus den eigenen Reihen kommt.



Woran erkenne ich Betrüger-Mails?

Cyber-Vertrauensschäden

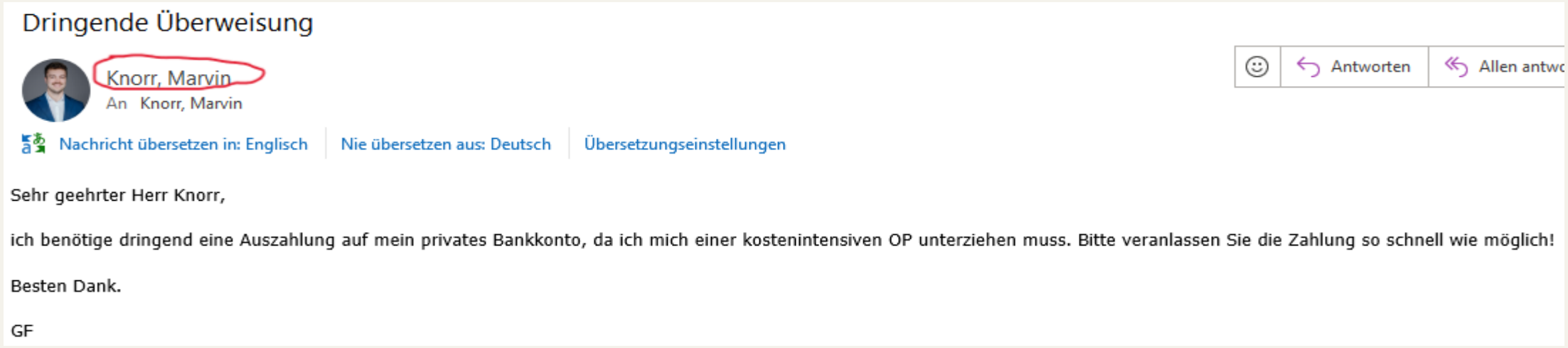


Die Domain – der Fingerabdruck im Internet

Jede Domain ist ein weltweit einzigartiger und eindeutiger Name für einen bestimmten Bereich des Internets

Erwartung? marvin.knorr@markel.de

Überprüfung: marvin.knorrr@markel.de, markel@marvin.knorr.de, marvin.knorr@markel.com



Cyber-Vertrauensschäden

Der Gang bei Markel

Erste (kurze) Deckungsprüfung: Besteht die Police, versicherter Zeitraum, versicherte Tätigkeit?

Während diesem Schritt prüfte BC bereits, ob sich der Betrüger möglicherweise Zugang zu den Systemen der VN verschafft hat. Zusätzlich musste geklärt werden, ob der Betrüger von außen oder aus den eigenen Reihen kommt.

... zurück zum Fall:

Betrüger Domain weicht von GF Domain ab.
BC: Betrüger kam von außen.

VN wurde geraten, Strafanzeige zu erstatten und die Überweisung durch die Hausbank stoppen zu lassen.

Teilbetrag konnte in England gestoppt werden.

Zweite Deckungsprüfung: Vertrauensschaden (+)
Nicht rückbuchbare Beträge wurden VN ersetzt

Cyber-Vertrauensschäden

Ausblick: DeepFake


Süddeutsche Zeitung

Ukraine Israel Politik Wirtschaft Meinung Panorama Sport München

> Digital > Technologie > Deepfake-Betrug: Angestellter überweist 24 Millionen Euro ins Nichts

Deepfake-Betrug

Angestellter überweist 24 Millionen Euro an Betrüger

5. Februar 2024, 14:46 Uhr | Lesezeit: 2 min | Kommentare


Videokonferenz voller KI-Klone: Angestellter schickt Betrügern 24 Millionen Euro

Bislang werden im Rahmen der "Chef-Masche" Angestellte zumeist von einer Person überzeugt, Geld herauszugeben. Ein Fall in Hongkong hat nun eine neue Qualität.


Merkur.de Ukraine-Krieg Politik Wirtschaft Deutschland Welt

Startseite › Leben › Karriere

Angestellter überweist Millionen an „Fake-Chefs“: So schützen Sie sich vor KI-Abzocke

08.03.2024, 11:13 Uhr

Verhalten im Schadenfall

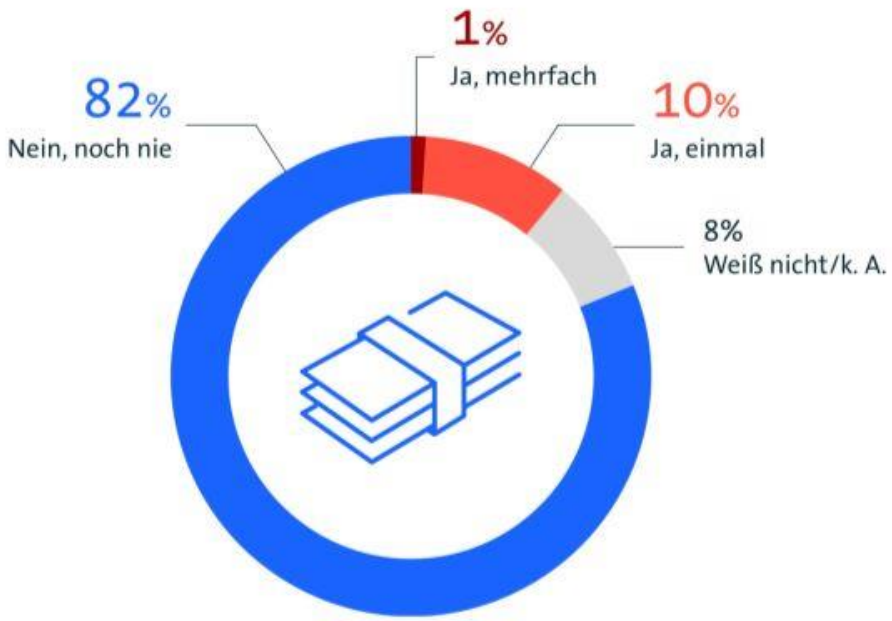
05

Ransomware-Angriff

Ransom-Verhandlungen und Zahlungen

Ransomware: Jedes neunte Opfer bezahlt Lösegeld

Haben Sie bei dem Ransomware-Angriff Lösegeld bezahlt?



Geschäftsbetrieb beeinträchtigt

Bei 4 von 10 Ransomware-Opfern (44 Prozent) kam es durch den Angriff zu Beeinträchtigungen im Geschäftsbetrieb. Im Durchschnitt dauerten diese rund 3 Tage.

Basis: Unternehmen, die von Ransomware-Angriffen betroffen waren (n=514) | Abweichungen von 100 Prozent sind rundungsbedingt. | Quelle: Bitkom Research 2023

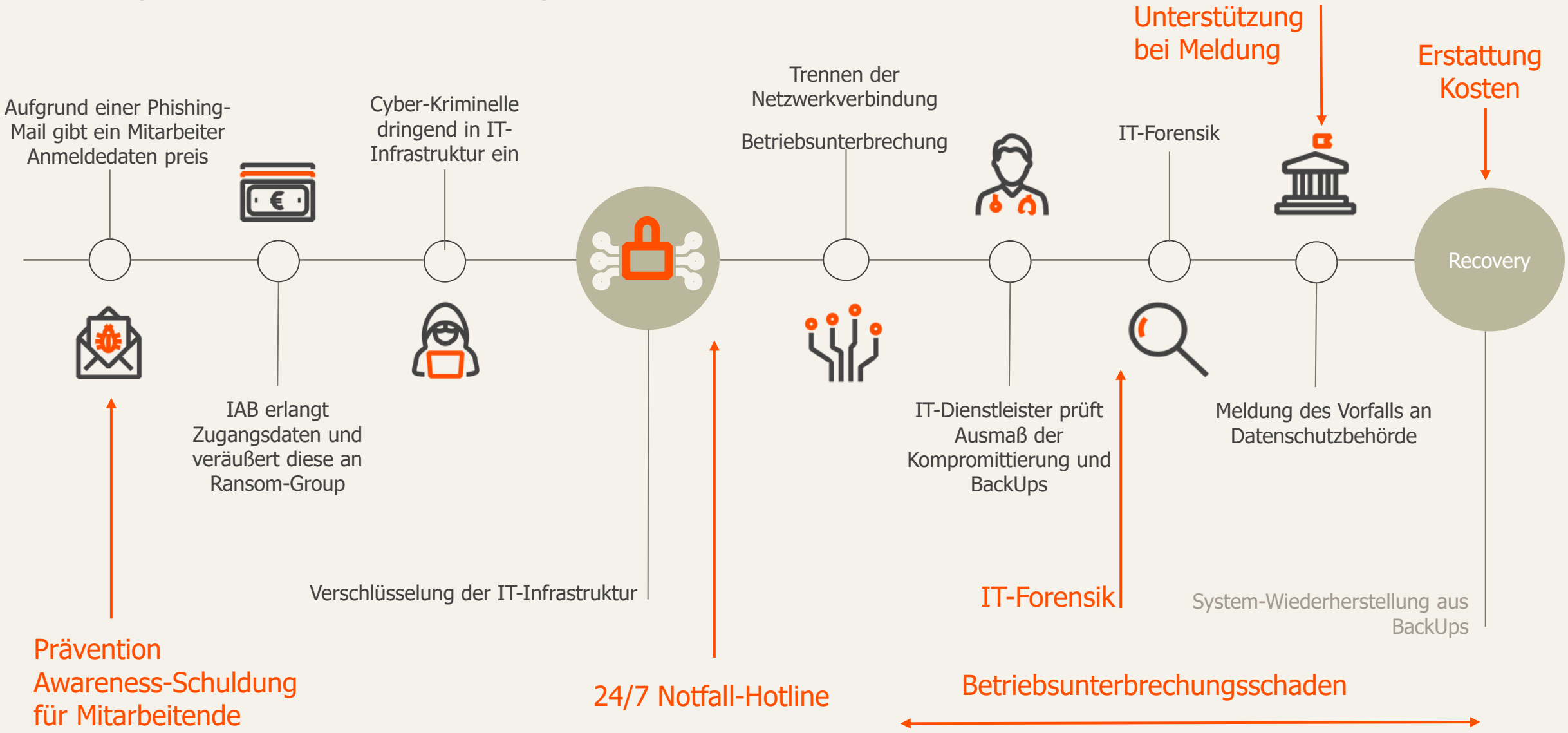
bitkom

Quelle: **Bitkom Research 2023**

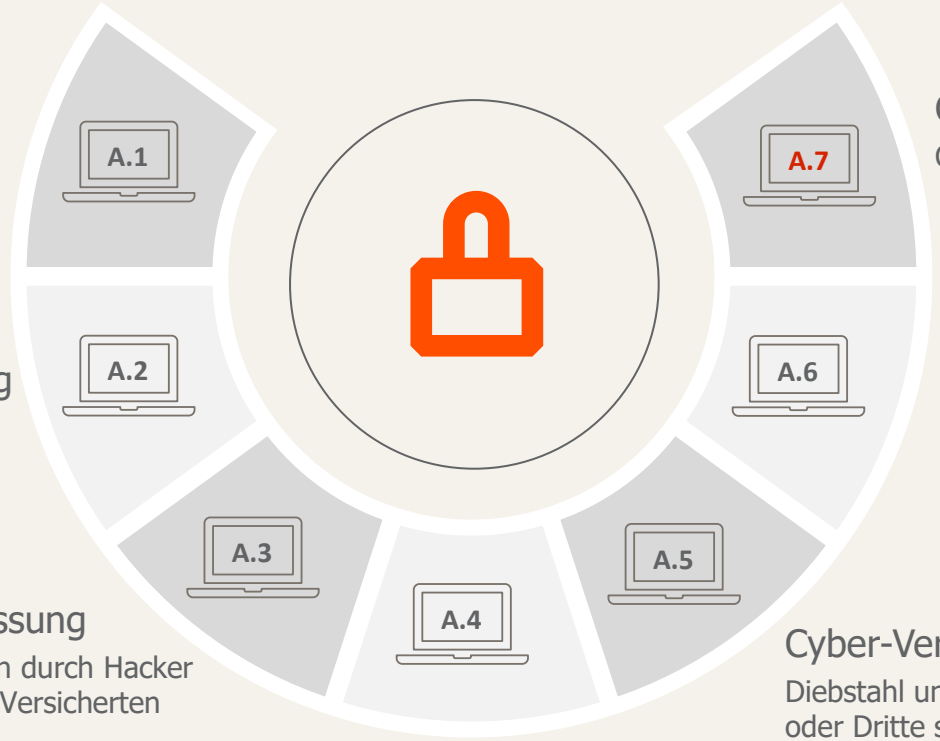
Maßnahmen im Schadenfall

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

Leistungen der Cyber-Versicherung im Schadenfall



Modularer Versicherungsschutz (Markel Pro Cyber v1)



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

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
heise online Videokonferenz voller KI-Klone (Videokonferenz voller KI-Klone: Angestellter schickt Betrügern 24 Millionen Euro | heise online)	2024	22
T3n.de (Wie ein Unternehmen 25 Millionen Dollar in einer Deepfake-Videokonferenz verlor (t3n.de))	2024	