Philipp Siglow – Underwriter Cyber

Cybercrime im KI-Zeitalter - neue Angriffe, neue Risiken, neue Antworten

MARKEL

Ihr heutiger Referent

Philipp Siglow

Underwriter Cyber

- Tätig in der Versicherungsbranche seit 2008
- Ausbildung zum Versicherungs- und Finanzkaufmann
- Vertriebs- und Führungspositionen bei Ergo und Generali

Beruflicher Werdegang bei Markel

- Key Account Manager im Bereich Business Development
- Haftpflicht Underwriter (DVA-zertifiziert)
- Spezialist im Bereich Cyber Underwriting

Die Cyber-Gefahrenlage

01

Markel Insurance in Deutschland

330.000

registrierte Fälle von Cybercrime in 2024 *

202 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 ****

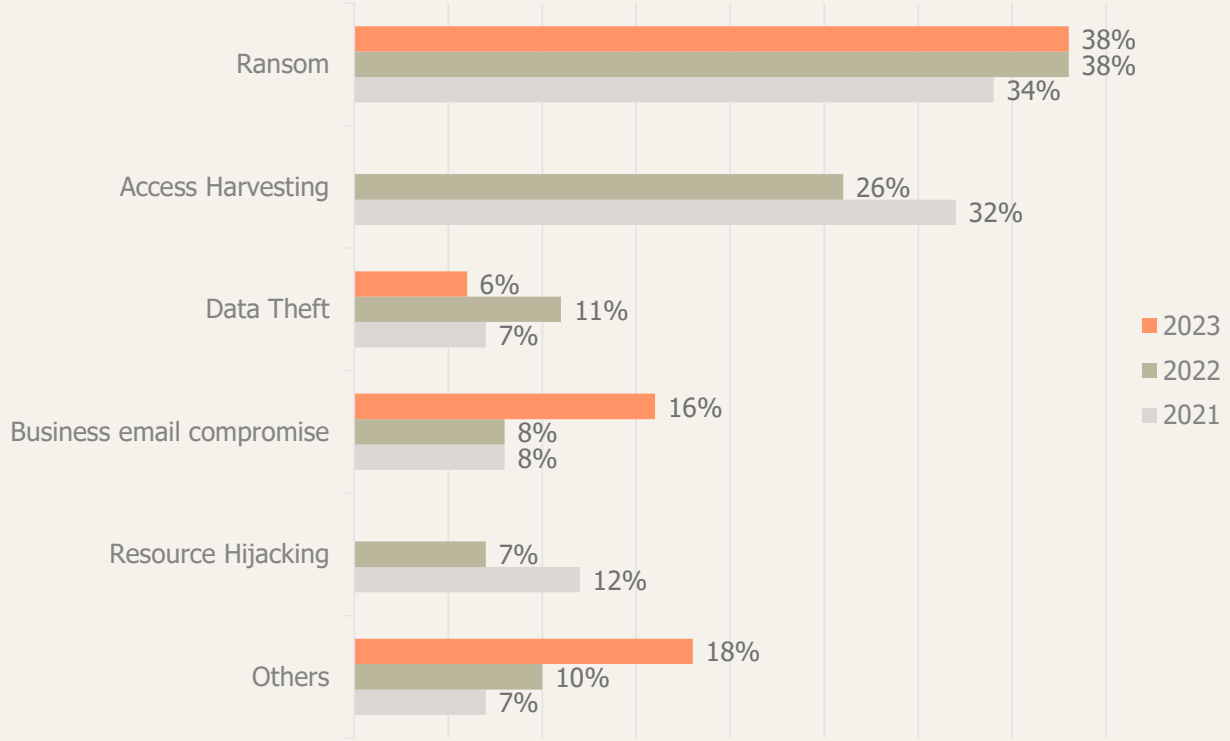
*BKA Bundeslagebild Cybercrime 2024

** TrueSec Threat Intelligence Report 2023

*** Bitkom Research 2025

**** Repräsentative Forsa-Umfrage unter 300 Entscheidungsträgern aus kleinen und mittleren Unternehmen im Mai/Juni 2023 (basierend auf Basis-Schutzmaßnahmen gemäß GDV-Richtlinien)

Arten von Cyberangriffen und deren Häufigkeit



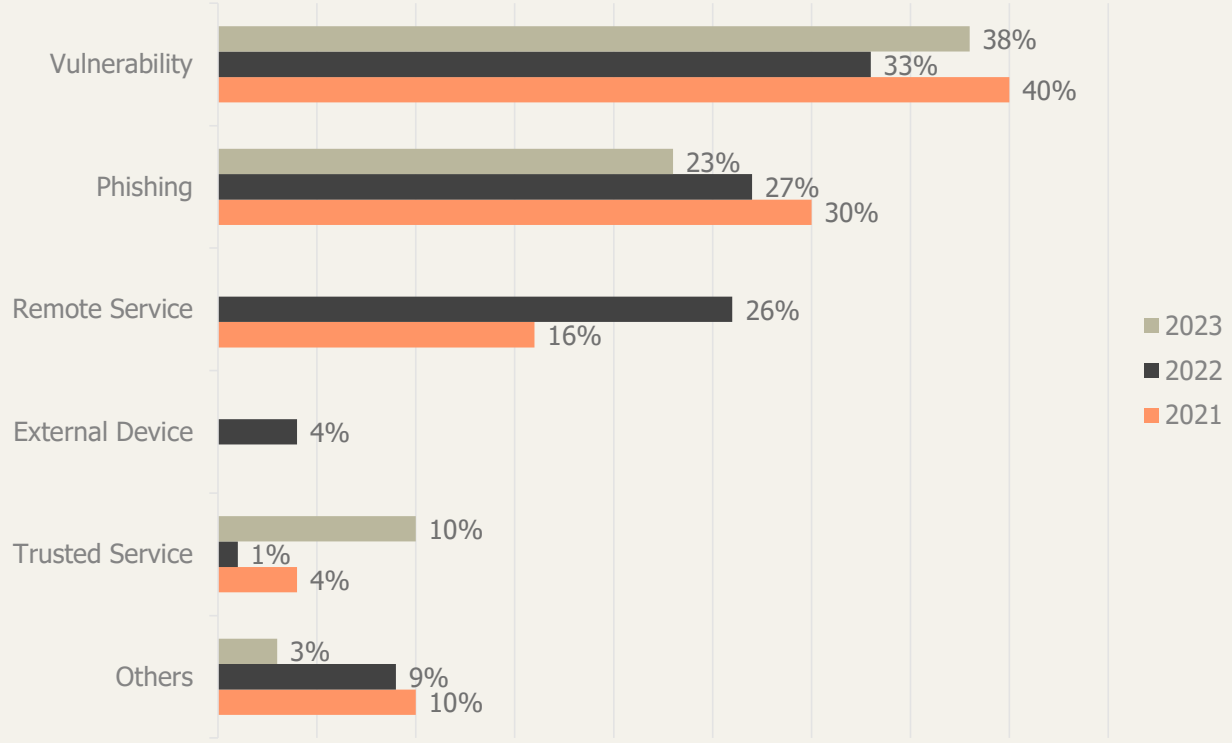
Quelle: **TrueSec Threat Intelligence Report 2024**

Angaben in Prozent

Cyber-Gefahrenarten

02

Angriffsvektoren / Einfallstore



Quelle: **TrueSec Threat Intelligence Report 2024**

Angaben in Prozent

Supply-Chain-Attack

- 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-Vertrauensschäden

Man-in-the-middle

Ein Angreifer greift unbemerkt die Kommunikation zwischen mehreren Parteien ab, verändert oder kontrolliert sie.

Phishing

Angreifer verwenden gefälschte E-Mails oder Webseiten, um Menschen dazu zu bringen, vertrauliche Daten preiszugeben.

Spoofing

Der Angreifer tarnt seine Identität, um sich als vertrauenswürdig darzustellen.

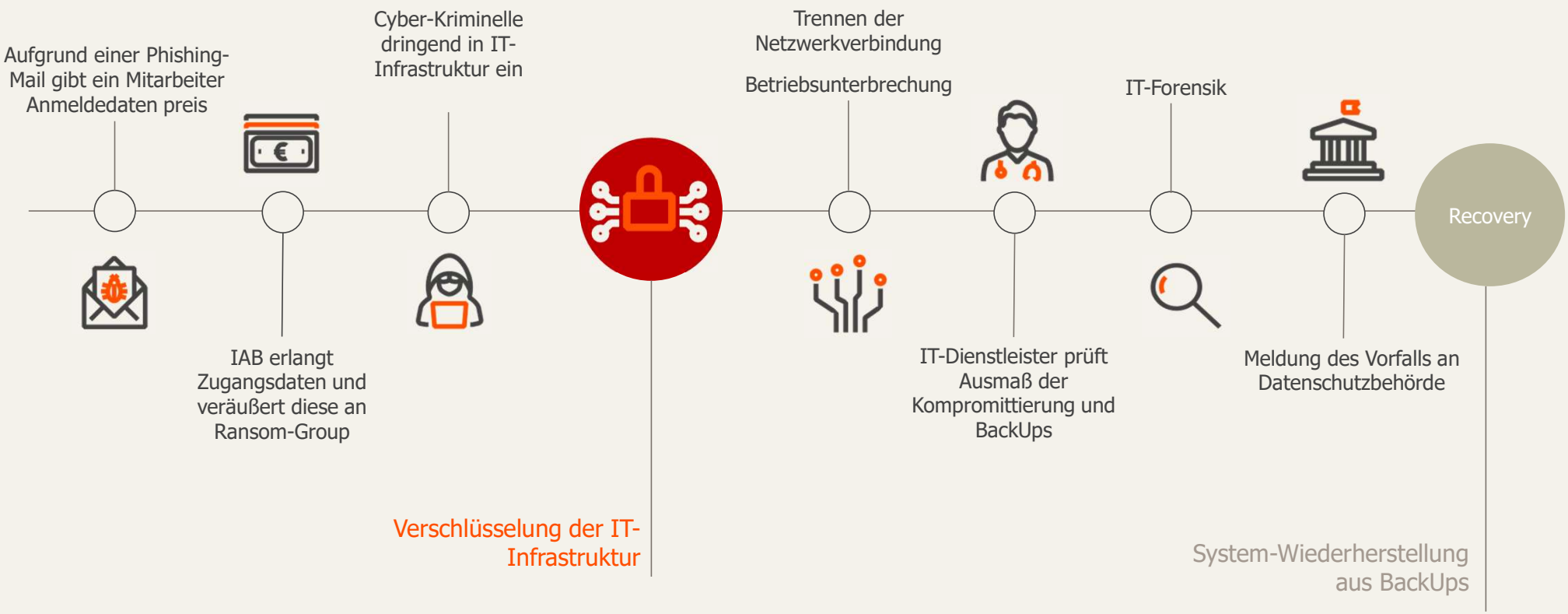
Fake President

Angreifer geben sich oft als Geschäftsführer aus, um Mitarbeiter zu Geldüberweisungen zu bewegen.

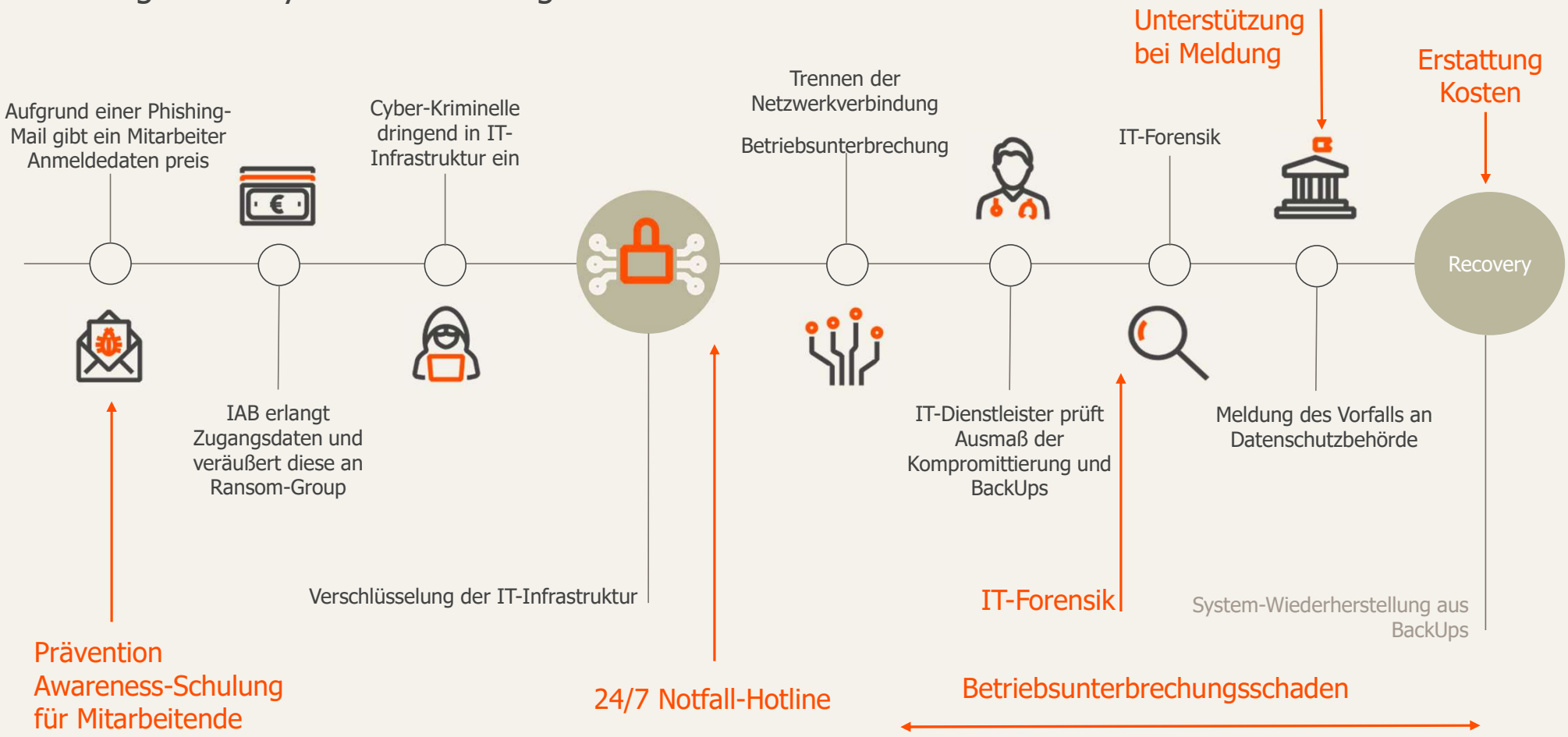
Schadensablauf: Ransom

03

(möglicher) Ablauf eines Ransomware-Angriffs



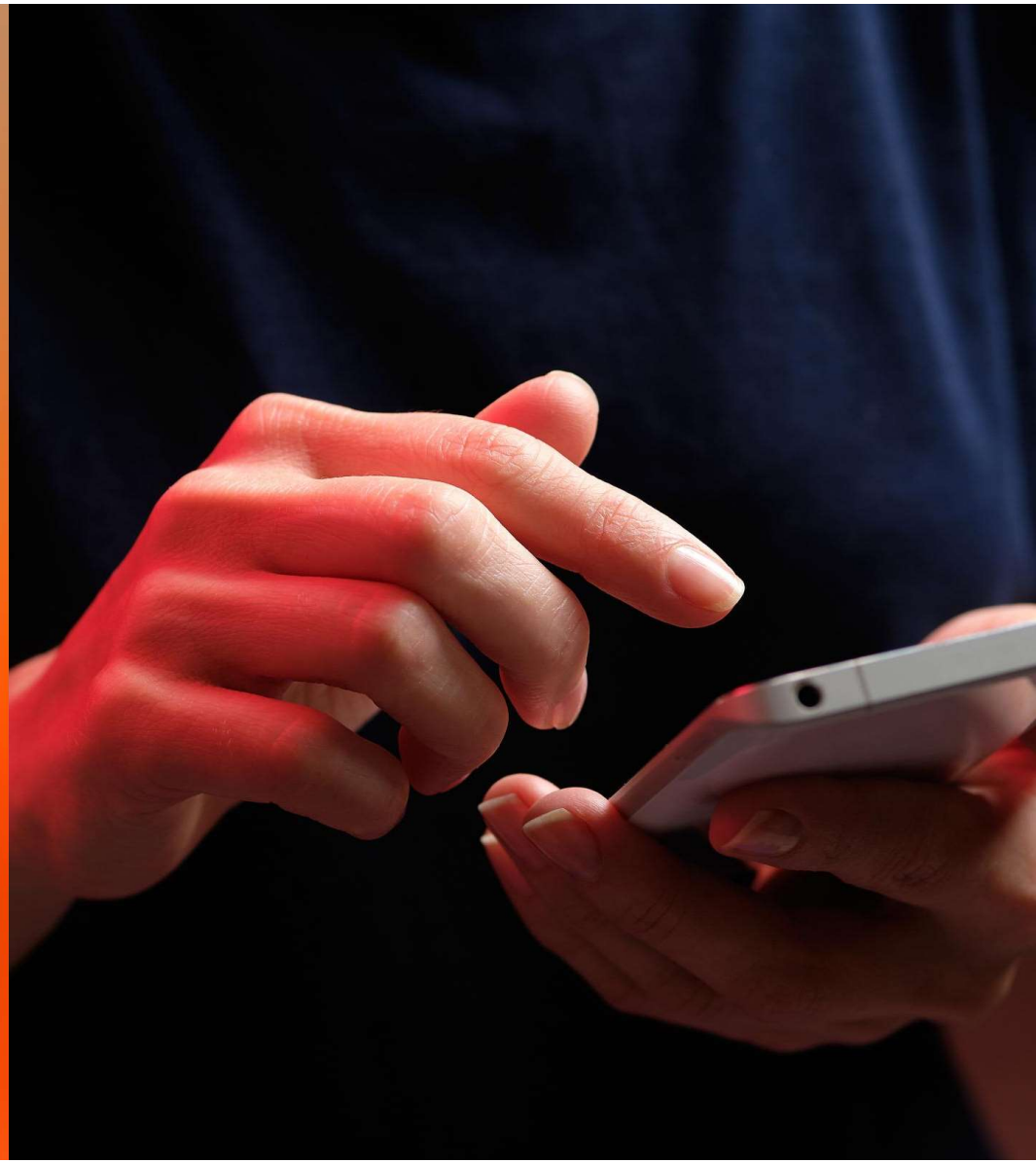
Leistungen der Cyber-Versicherung im Schadenfall



Was leistet eine Cyber-Versicherung im Schadenfall

01 Sofortmaßnahmen	Technischer Support leistet Unterstützung bei Sofortmaßnahmen
02 IT-Forensik	Kostenerstattung für geeignete IT-Forensik, zur Aufklärung der Kompromittierung
03 System-Wiederherstellung	Kostenerstattung für IT-Dienstleister zur Wiederherstellung der Sicherheit der Systeme
04 Erstattungszahlungen	z.B. bei versicherten Falschüberweisungen nach Cyber-Betrug
05 Ertragsausfall nach Betriebsunterbrechung	erleidet der Betrieb aufgrund eines Cybervorfalles Ertragsausfälle, werden diese durch den Versicherer erstattet

Ransomeware
Deepfakes
Phishing



04

Ransomware-Angriff

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

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

Mitarbeiterin

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

KONTOBEZEICHNUNG: [redacted]
ADDRESSE: [redacted]
IBAN: [redacted]
BIC: [redacted]
SC: [redacted]
KONTO NUMMER: [redacted]
BANK: [redacted]
ZWECK: [redacted]
REFERENZ: [redacted]

...Senden mir den Überweisungsbeleg.

Grüße,
[redacted]

Von: [redacted]
Gesendet: Dienstag, 26. September 2023 08:13
An: [redacted]
Betreff: AW: [redacted] Mitarbeiterin

Guten Morg[redacted] Geschäftsführerin

anbei der Überweisungsbeleg 😉
Ich habe Ihre Mail ger[redacted] Geschäftsführerin n und gleich ausgeführt.

Viele Grüße
[redacted]

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).

Cyber-Vertrauensschäden

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

Arten von Deepfakes

Video-Deepfakes	Audio-Deepfakes	Bild Deepfakes	Kombinationen
Gesichtsaustausch (Face Swap) Täuschend echter Identitätswechsel in Videos. **Lippen-Synchronisation** Manipulation von Reden oder Aussagen.	**Voice Cloning** Täuschung durch nachgemachte Stimmen z.B. CEO-Betrug	**Realistische Standbilder** für Fake-Alibis oder soziale Netzwerke. **Biometrische Bilder** können nachgeahmt oder manipuliert werden.	**Audio-Video-Deepfakes** Täuschend echte Videokonferenzen. **Multimedia-Manipulationen** Bilder, Videos und Audio kombiniert.

Deepfakes in der Praxis

Deepfake-Betrug

Angestellter überweist 24 Millionen Euro an Betrüger

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

Deepfake

Hier spricht der Ferrari-Chef – nicht

29. Juli 2024, 12:32 Uhr | Lesezeit: 2 Min. | 6 Kommentare

DDOS als Software

Malware as a Service

→ Rent a Botnet
- „Pay per attack"
- Günstig: Wettbewerb zwischen den Anbietern führt zu
- Zahlung über Paypal / Bitcoin

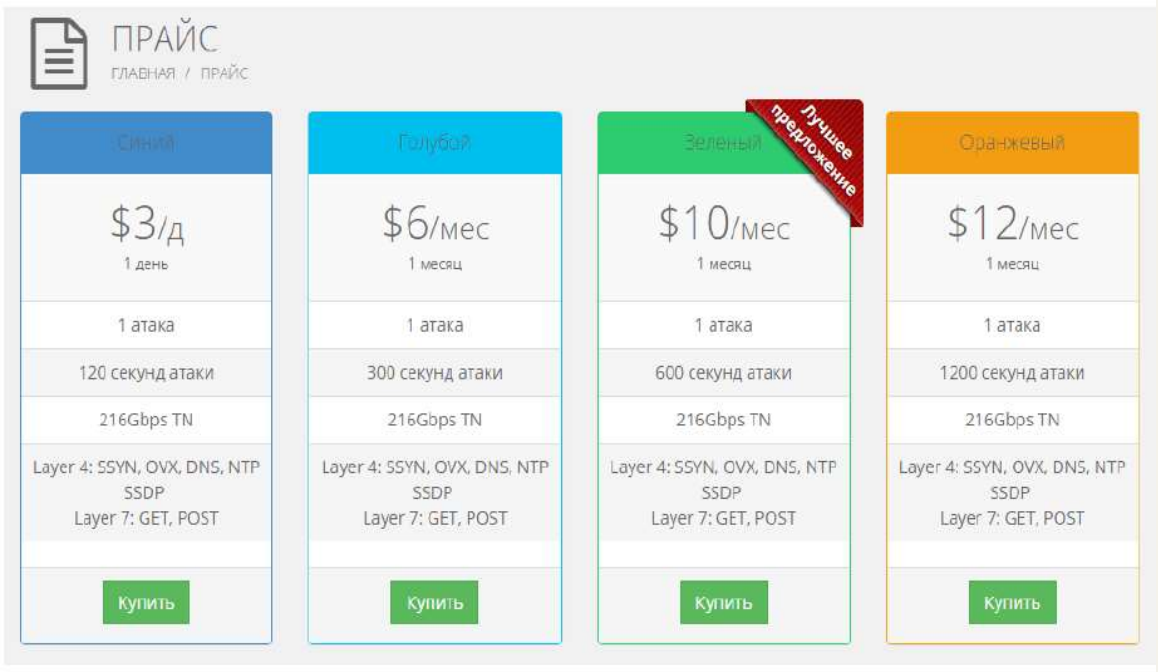
Spezifikationen sind standardisiert

→ Angriffsziele

→ Dauer der Attacke

→ Zahlung über Paypal / Bitcoin

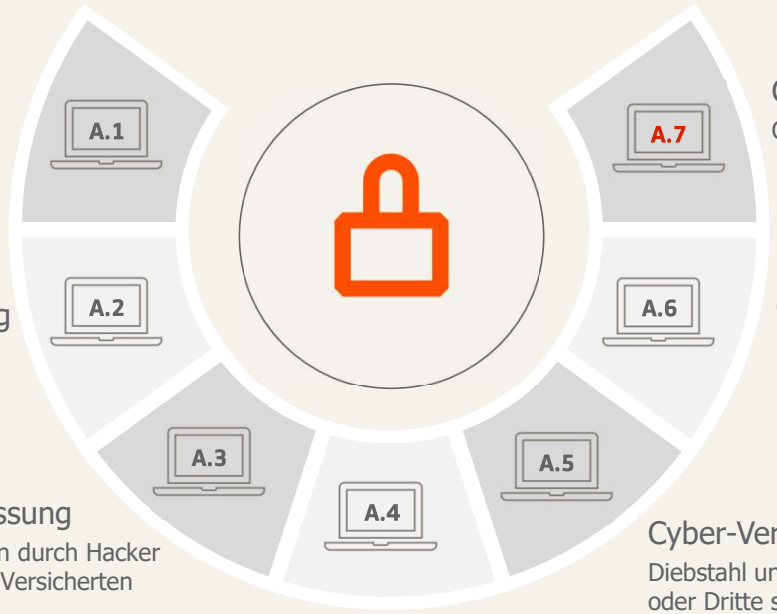
→ Art des Angriffes



Markel
Pro Cyber v2

05

Markel Pro Cyber v2



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

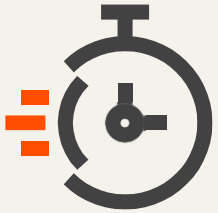
A.1 Cyber Daten- und Eigenschäden – (Grunddeckung und Pflichtmodul)

Umfasst unter anderem:

- Sofortige Unterstützung bei begründetem Verdacht (24 Stunden, 7 Tage die Woche)
- Wiederherstellung von IT-Systemen, Programmen und Daten
- Information der betroffenen Personen
- Maßnahmen im Bereich Public Relations und Reputationsmanagement
- Durchführung von Sicherheitsanalysen und Optimierung der Sicherheitsmaßnahmen
- Zusätzliche steuerliche Aufwendungen

A.2 Cyber-Betriebsunterbrechung

Keine Haftzeit !



Umfasst unter anderem:

- Cyber-Betriebsunterbrechungen bei Einsatz von Cloud- und Hosting-Diensten
- Cyber-Betriebsunterbrechungen aufgrund behördlicher Anordnungen durch Datenschutzbehörden
- Cyber-Betriebsunterbrechungen infolge technischer Störungen
- Vorleistungen im Zusammenhang mit der Nutzung von Cloud- und Hosting-Diensten

A.3 Cyber-Erpressung

Umfasst unter anderem:

- Die Erstattung des gezahlten Betrags
- Den Ersatz der gelieferten Ware oder erbrachten Dienstleistung
- Prämienzahlungen

A.4 Cyber-Zahlungsmittel

Versicherungsschutz bei Verstößen gegen

- Vertragliche Verpflichtungen aus Kreditkartenverarbeitungsvereinbarungen mit Kreditinstituten,
- Weitere Vereinbarungen im Zusammenhang mit anderen Zahlungssystemen, wie etwa Bankkarten (EC-Karten),
- Vereinbarungen mit Zahlungsprozessoren und E-Payment-Anbietern, die den Schutz personenbezogener Daten gemäß § 3 Absatz 1 BDSG oder vergleichbarer ausländischer Rechtsvorschriften zum Ziel haben, infolge von Cyber- und Daten-Eigenschäden.

A.5 Cyber-Vertrauensschaden

Vertrauensschäden durch interne Mitarbeiter

- Betrug
- Urkundenfälschung
- Unterschlagung
- Diebstahl von Firmengeldern, Kundendaten, Waren und Ähnlichem

Vertrauensschäden durch externe Dritte

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

Darüber hinaus sind auch Schäden durch Fake President und andere Formen des Social Engineering versichert.

A.6 Cyber-Haftpflicht

Umfasst unter anderem:

- Verstöße im Bereich der Cyber-Sicherheit, insbesondere die Verbreitung von Schadsoftware
- Datenschutzverletzungen
- Verstöße gegen Geheimhaltungspflichten
- Verletzungen von Namens- und Persönlichkeitsrechten
- Verstöße im Zusammenhang mit Werbung und Marketing
- Haftungsfreistellung für externe Datenverarbeiter

Cyber Prävention

06

Wie kann ich mich vor Cyber-Angriffen schützen

Benennen Sie einen Hauptverantwortlichen für die IT-Sicherheit.

- Sensibilisierung der Geschäftsführung sicherstellen
- Verantwortlichkeiten für die Durchführung der Maßnahmen definieren

Erfassen Sie ihre IT-Systeme.

Aufstellung der
- verwendeten Software
- verarbeiteten Daten und deren Verarbeitung
- gewährten Zugriffsrechte
- IT-Schnittstellen zur Außenwelt

Führen Sie regelmäßige Datensicherungen durch.

- Bestimmen Sie die zu sichernden Daten
- Definieren Sie die Häufigkeit der Datensicherung
- Entscheiden Sie sich für ein passendes Speichermedium zur Sicherung der Daten

Wie kann ich mich vor Cyber-Angriffen schützen

Führen Sie Updates durch.

- Setzen Sie moderne Hardware- und Softwaretechnologien ein
- Stellen Sie automatische Aktualisierungen sicher
- Bestimmen Sie die verantwortliche Person für den Update-Prozess

Deaktivieren Sie Makros.

- Makros sind kleine Programme, die sich beispielsweise in Word-, Excel-, PowerPoint- oder PDF-Dateien integrieren lassen.

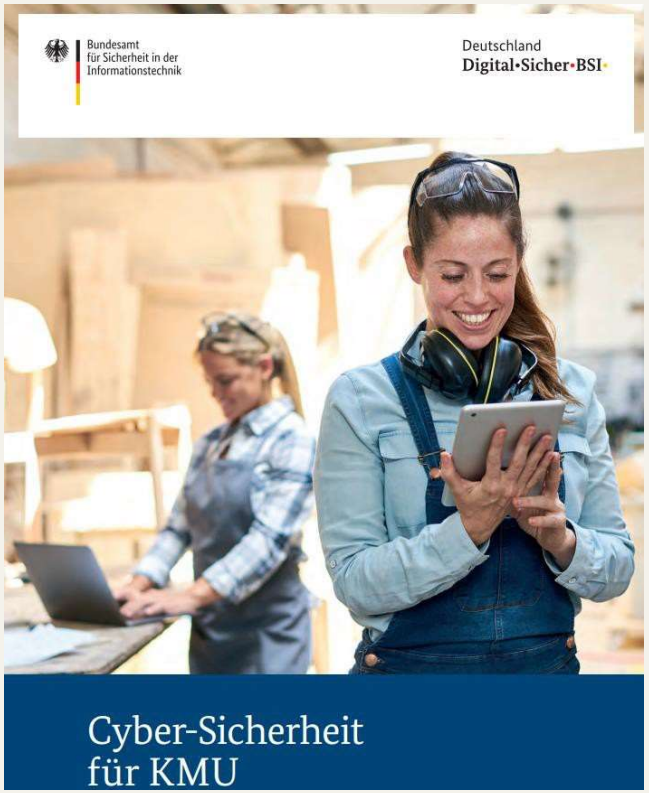
Nutzen Sie Virenscanner und Firewalls.

- Kompatible Installation auf sämtlichen Systemen

Legen Sie eine Richtlinie für Passwörter fest.

- Implementierung der Multi-Faktor-Authentifizierung (MFA)
- Festlegung einer Mindestanzahl an Zeichen

Empfehlung Cyber-Sicherheit für KMU – Die Top 14 Fragen




MARKEL