

Wie Sie mit dem Management von Privilegien den Anforderungen von Cybersicherungen gerecht werden

29. September 2022



Detlef Lüke
Solutions Engineer



Agenda

- Cyberversicherung – Definition
- Der Markt für Cyberversicherungen
- Cyberversicherungen – Aktuelle Lage
- Ausblick in die Zukunft
- Umsetzung der geforderten Kriterien für Cyberversicherungen



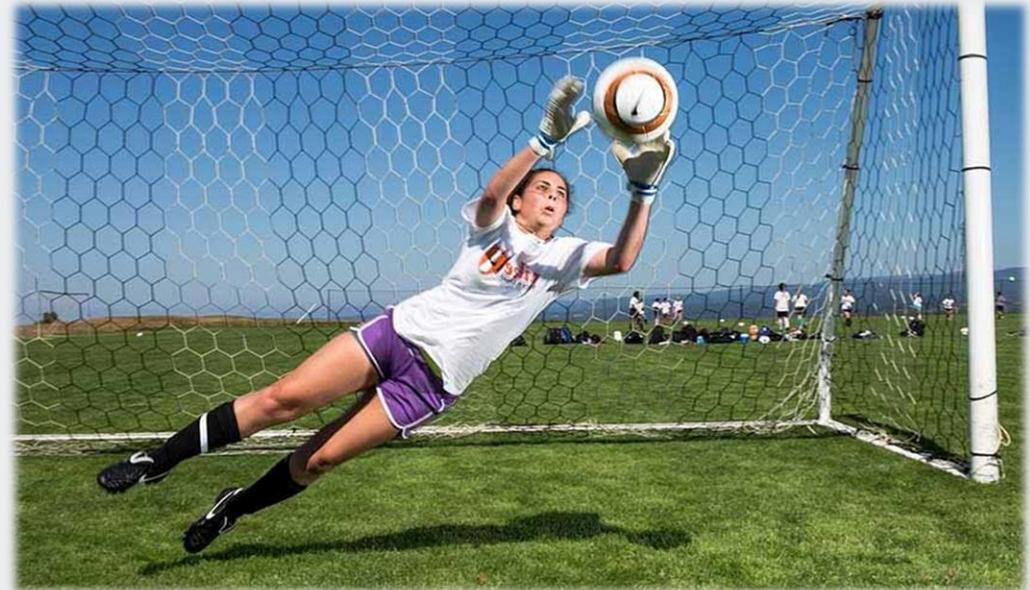
Cyberversicherung

– Definition

Was ist eine Cyberversicherung?

Eine **Cyberversicherung** ist eine Zusatzversicherung für Unternehmen, die Schäden im Zusammenhang mit Hacker-Angriffen oder sonstigen Akten von Cyberkriminalität absichert.

- Drittschäden (Haftpflicht)
- Eigenschäden



Eventuelle Ausschlüsse

- Allgemeine Haftung
- Gewerbliches Eigentum
- Schadenersatzansprüche aus Arbeitsverhältnissen
- Berufshaftpflicht
- **Rechtsstreitigkeiten zu Systemanfälligkeiten vor einer Datenschutzverletzung:** Bei Systemanfälligkeiten vor einem Verstoß decken Cyberversicherungen damit verbundene Klagen nicht ab.
- Zukünftige Gewinneinbußen
- Diebstahl geistigen Eigentums
- Kriegshandlungen
- Technologische Verbesserungen
- **Social-Engineering-Angriffe:** Geschäftliche Cyberversicherungen decken keine Phishing- oder Social-Engineering-Angriffe ab. Private Cyberversicherungen dagegen umfassen häufig Schäden durch Phishing-Attacken.



Cyberversicherungen

– Der Markt



Der Markt für Cyberversicherungen steht Kopf

Cybervorfälle, Angriffe und aktuelle Veränderungen:
Auswirkungen für Unternehmen und Geschäftsaussichten



Wichtige Markttreiber

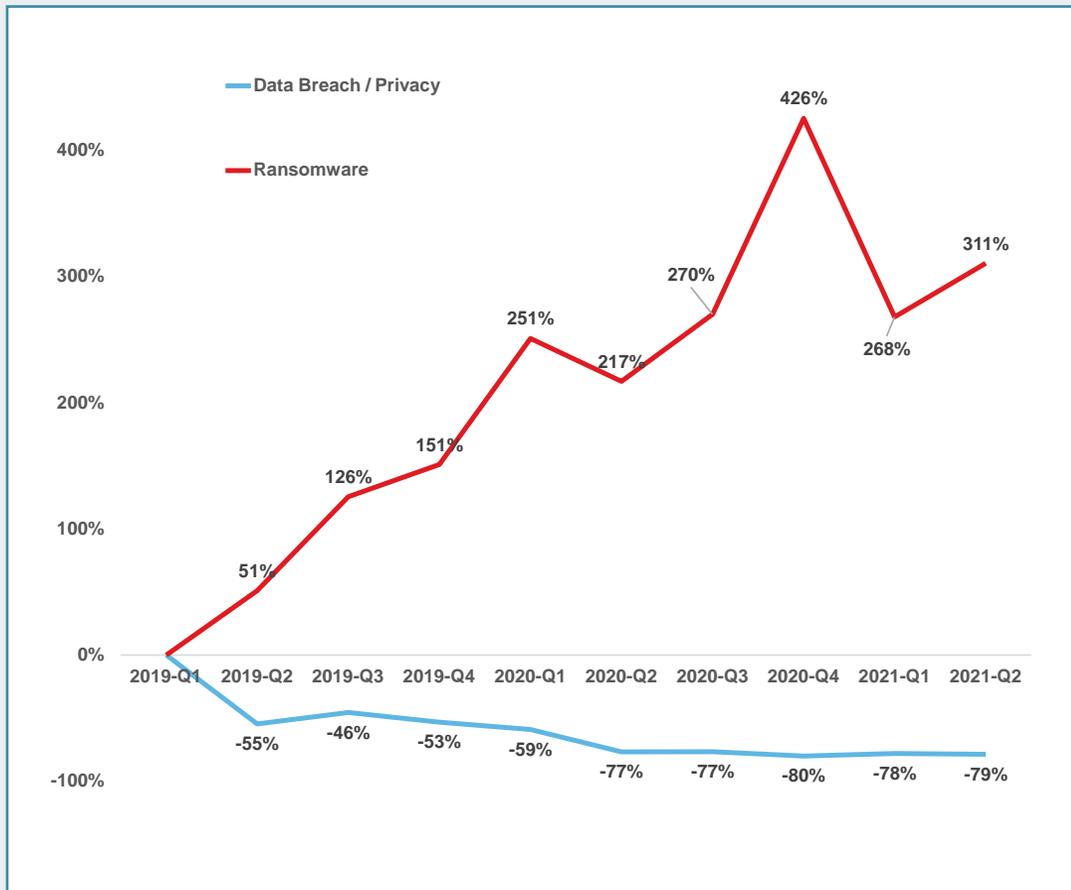
Digitale
Transformation

Remote Work /
Corona-Pandemie

Gesetzesvorgaben
und Geldbußen

\$ CYBER-KRIMINALITÄT IST BIG BUSINESS \$

Häufigkeit von Cyberfällen im Zeitverlauf



*Percent change relative to 2019-Q4

Quelle: Risk Based Security, analysis by Aon. Data as of 7/12/2021; Ransomware data exfiltration and downtime per Coveware Quarterly Ransomware Report as of 4/26/2021

Ransomware-Aktivitäten
übertreffen deutlich die Zahl
der Datenschutzverletzungen

311%

Durchschnittliche
Ausfallzeiten durch
Ransomware-Attacken

23

Daten-Exfiltration bei
Ransomware-Attacken

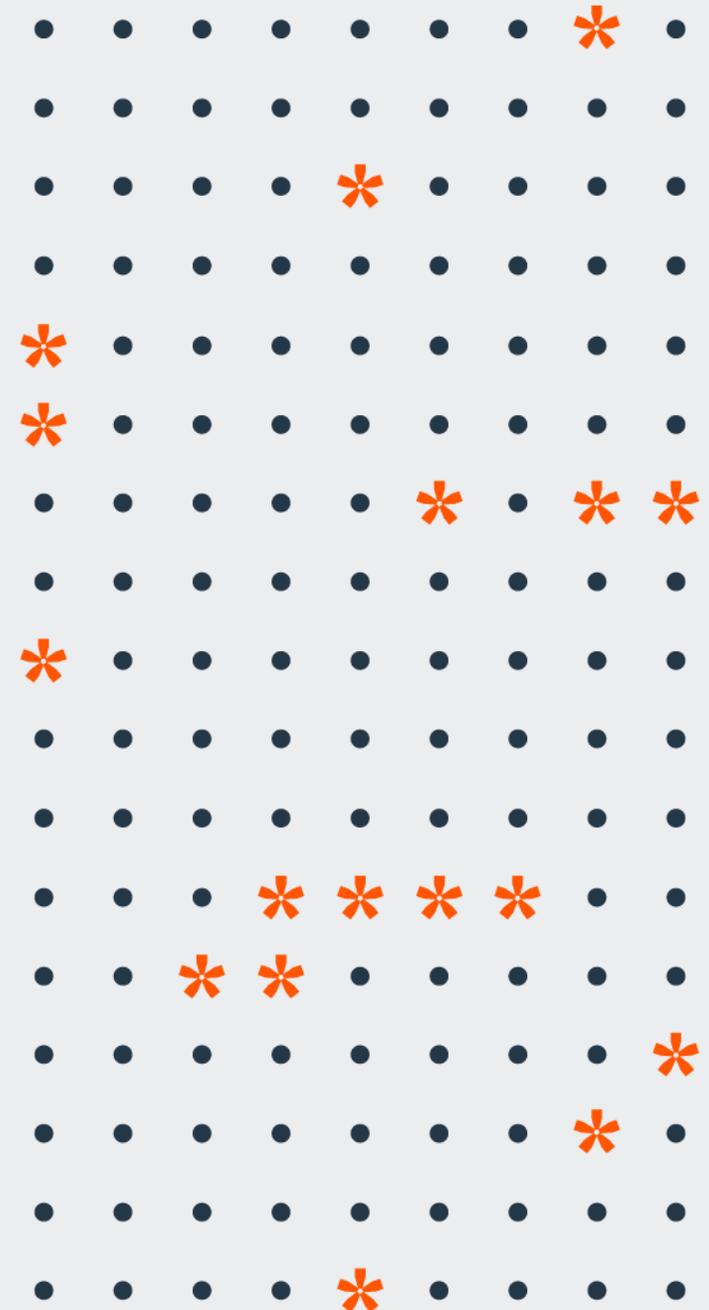
77%

Geschäftsunterbrechungen
als größter Schadensfaktor

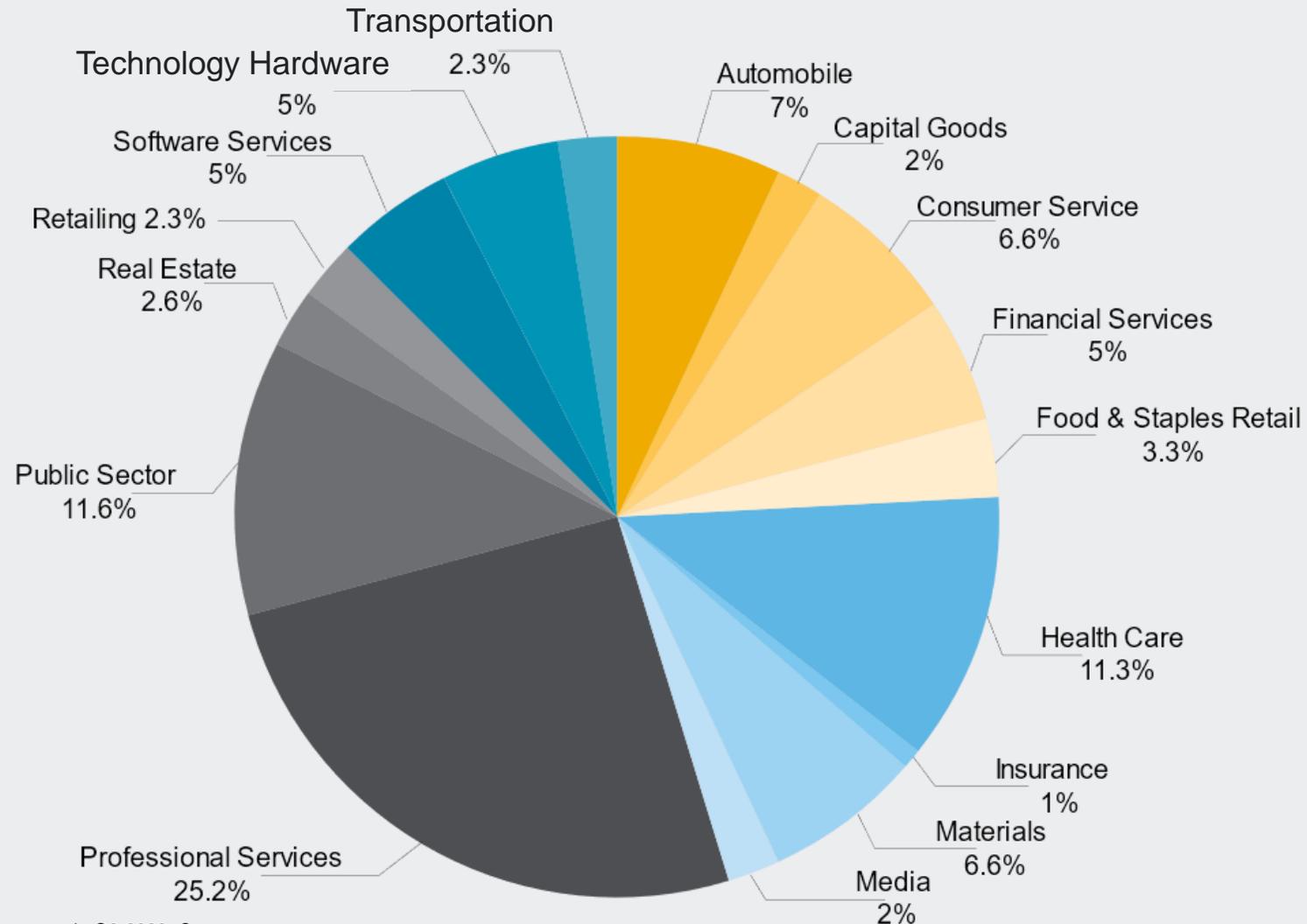
Achtstellige
Verluste

Wer ist am stärksten betroffen?

DIE STATISTIKEN KÖNNTEN SIE ÜBERRASCHEN

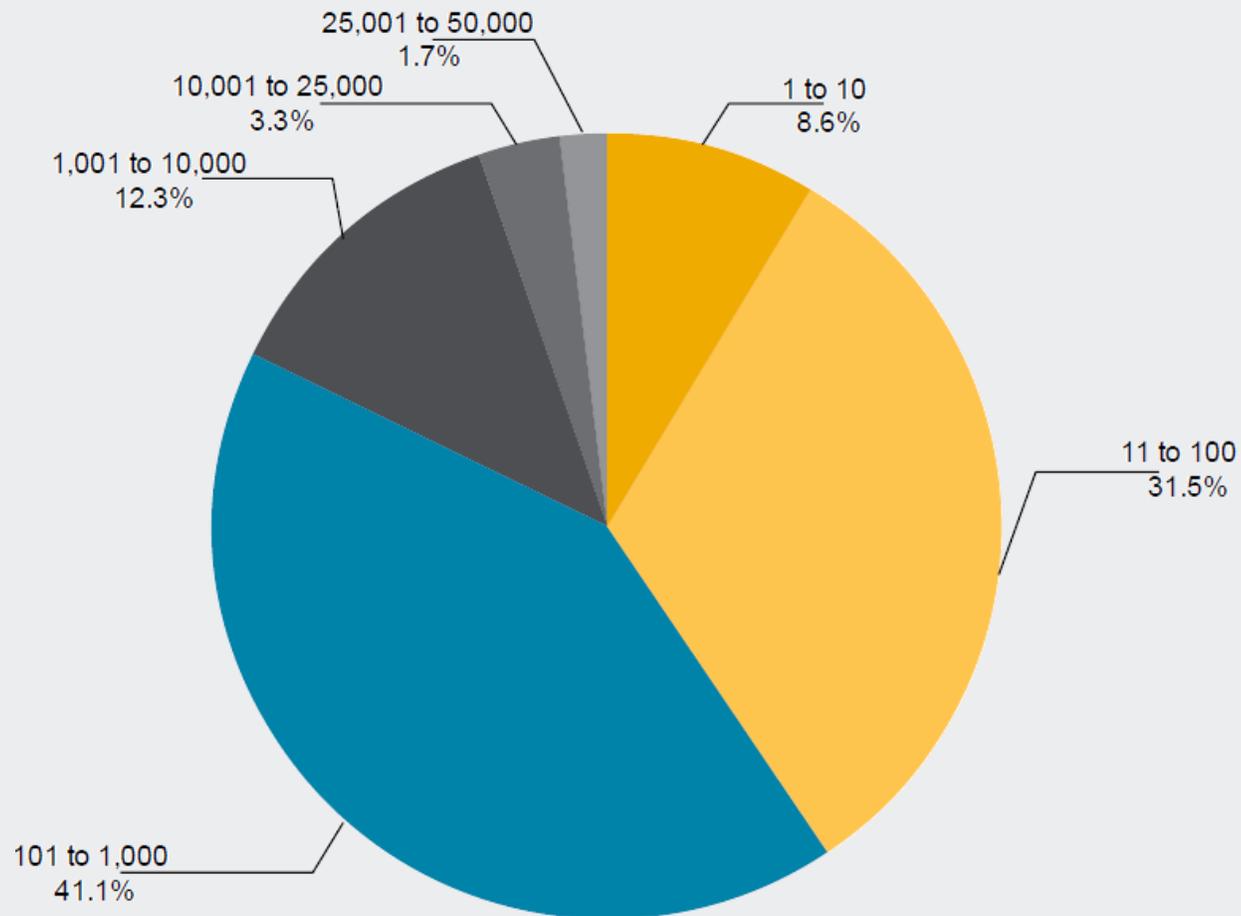


Angriffsziele im Branchenvergleich



Quelle: Common Industries Targeted by Ransomware in Q3 2020, Coveware

Gezielte Angriffe nach Firmengröße



- Unternehmen mit bis zu 1.000 Mitarbeitern sind von **81%** der Angriffe betroffen
- *Die Gründe?* Kleine und mittlere Unternehmen haben niedrigeren Reifegrad bei der Cybersicherheit.



Cyberversicherungen

– Aktuelle Lage

Cyberversicherungen machen erstmals Verluste...

| Jahr | Anzahl Versicherungsunternehmen | Beiträge ¹ | | Leistungen ² | | Schaden-Kosten-Quote ³ |
|------|---------------------------------|-----------------------|--------------------------|-------------------------|--------------------------|-----------------------------------|
| | | in Mio. EUR | Veränderung ggü. Vorjahr | in Mio. EUR | Veränderung ggü. Vorjahr | |
| 2020 | 33 | 106 | 39,0% | 37 | 59,0% | 64,7% |
| 2021 | 39 | 178 | 49,2% ⁴ | 137 | 187,6% ⁴ | 123,7% |

- Beiträge steigen um knapp 50 %
- Leistungen haben sich fast vervierfacht
- Einnahmen von 100 Euro standen Ausgaben von 123 Euro gegenüber

...und beklagen stagnierendes IT-Sicherheitsniveau

Der GDV-Hauptgeschäftsführer fordert insbesondere mittelständische Unternehmen auf, sich stärker gegen Cyberattacken zu wappnen.

„Die Angriffe werden immer professioneller und häufiger, aber das Niveau der IT-Sicherheit stagniert seit Jahren.“

Der Mittelstand habe die Potenziale bei der Prävention bei Weitem noch nicht ausgeschöpft: „Wir sehen bei den meisten Unternehmen noch große Sicherheitslücken“

Die Versicherungswirtschaft könne mit Cyberversicherungen das Restrisiko eines erfolgreichen Angriffs absichern – ein solcher Schutz setze aber ein gewisses Maß an IT-Sicherheit voraus.



Cyberversicherungen

– Ausblick

Auswirkung von Cyberversicherungen



Policen

Kunden

Ausschluss von Risiken

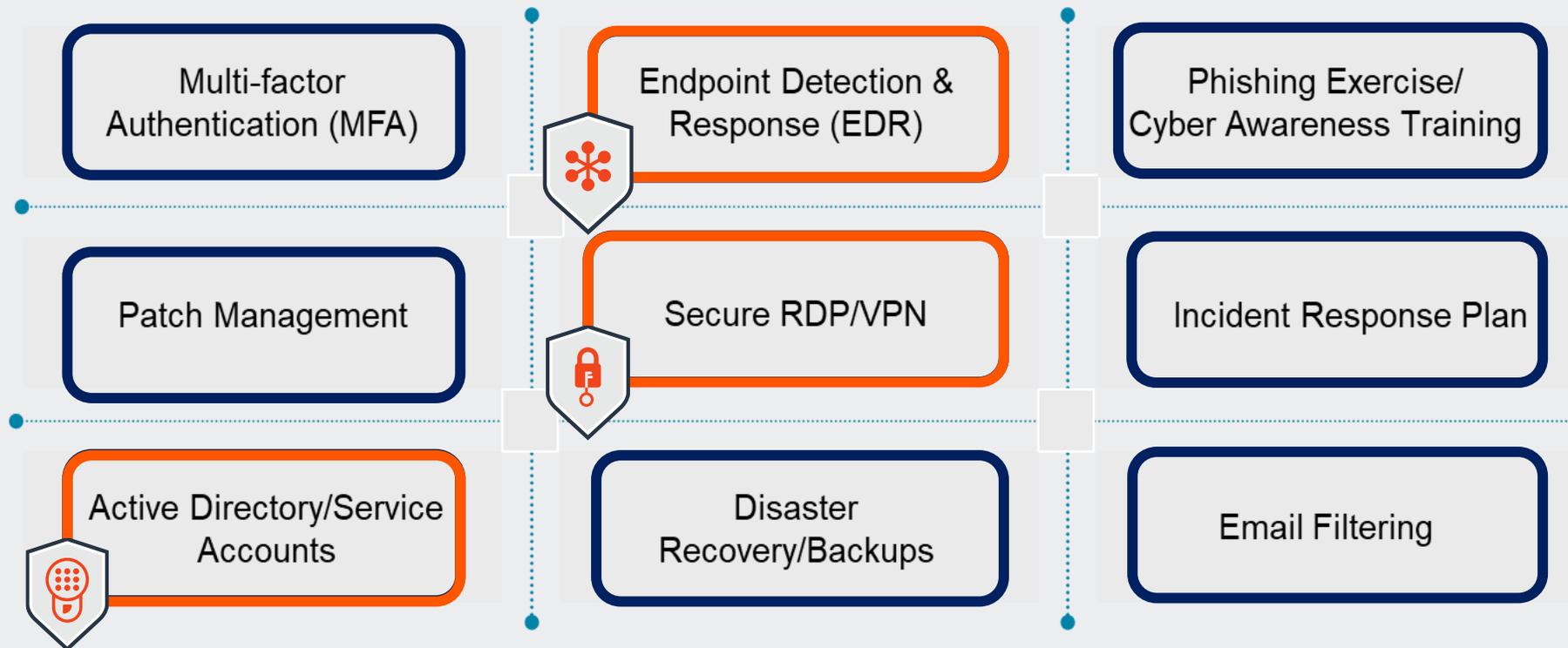
"Selbstbeteiligung"

Höhere Policen

Scanning / Probing

Risikobewertungen

Neun Security-Anforderungen, auf die Versicherungen achten





Cyberversicherungen

– Kriterien und Privilege Management

PAM setzt geforderte Kriterien für Cyberversicherungen um

Was müssen Sie bei Ihrer Cyberversicherung beachten?
Gibt es Anforderungen oder Fristen, die Sie einhalten müssen?

Schutz der Zugangswege

- Management von Sitzungen
- Dienstkonten
- Privilegierte Zugänge

Endpunktsicherheit

- Durchsetzung von Standardbenutzerrechten
- Unterbrechung von Angriffsketten
- Applikationskontrolle und Lizenzsteuerung

Entfernung von Remote-Work-Risiken

- Kein VPN
- Jump Host/Bastion-Kontrolle
- Punkt-zu-Punkt-Verschlüsselung

Cloud-Privilegien-Einsatz

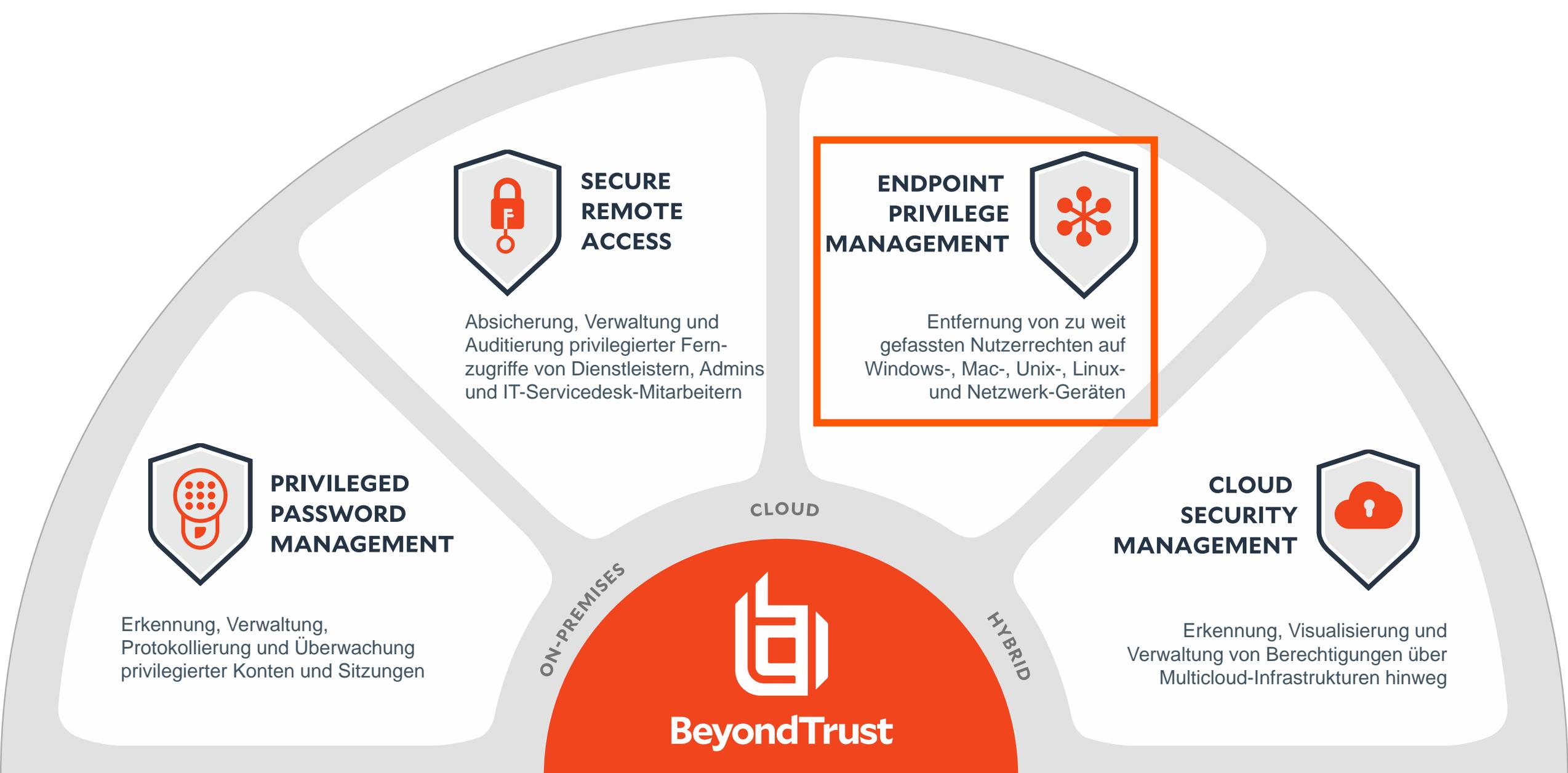
- Multicloud-Sicherheitsmanagement
- eDiscovery
- Verantwortlichkeiten

Sie benötigen Hilfe?

BeyondTrust-Lösungen für Privileged Access Management (PAM) bieten **spezifische Sicherheitsfunktionen, die Cyberversicherer einfordern.**

- Durchsetzung von Least-Privilege-Vorgaben
- Privilegiertes Konten- und Zugangsdatenmanagement
- Remote-Access-Sicherheit
- Malware- und Ransomware-Schutz
- Sicherheit gegen externe und interne Bedrohungen (egal, ob vorsätzlich oder unbeabsichtigt)







Endpoint Privilege Management

Entfernung von zu weit gefassten Nutzerrechten auf Windows-, Mac-, Unix-, Linux- und Netzwerk-Geräten

Schnelle Erreichung von Least-Privilege

Entfernung lokaler Adminrechte auf allen Endpunkten und schnelle Wertschöpfung mit sofort verfügbaren Quick Start Policies

Stopp von Phishing, Ransomware und Malware

Reduzierung der Angriffsfläche durch die **bedarfsgesteuerte Zuweisung von Just-in-Time-Privilegien** für autorisierte Anwendungen, Skripte, Aufgaben und Befehle

Einhaltung von IT-Compliance-Vorgaben

Einhaltung interner und externer IT-Compliance-Anforderungen durch **Entzug von zu weit gefassten Privilegien, Einsatz von Applikations-Whitelisting** und gesetzeskonforme Protokollierung der Nutzeraktivitäten

Kostenlose Testversion

Privilege Management für Windows und Mac



Kostenlose Cyberversicherungs- Checkliste

Cyberbedrohungen und Ransomware-Angriffe zwingen Anbieter von Cyberversicherungen dazu, strengere Anforderungen an die Versicherungsnehmer zu stellen.

Nutzen Sie unsere Checkliste zur Orientierung

The graphic features an orange header with the BeyondTrust logo and a decorative pattern of white squares. Below the header, the title 'Meet Insurance Requirements with PAM Cybersecurity Insurance Checklist' is displayed in bold. A woman in a black blazer stands behind a white desk, with a laptop and a checkmark icon visible. The background includes a pattern of black dots and a checkmark icon.

BeyondTrust

Meet Insurance Requirements with PAM
**Cybersecurity
Insurance Checklist**

The blistering pace and expanding scope of cyberthreats and ransomware attacks is forcing cyber insurance companies to steeply increase their rates and premiums, and even drop coverage for high-risk organizations. Underwriting requirements to be approved for cyber insurance are becoming more stringent.

BeyondTrust Privileged Access Management (PAM) solutions provide the foundational security that cyber insurers demand for reducing risk and liability, from external and internal cyber threat actors.

Our products enable essential capabilities, such as least privilege enforcement, privileged account and credential management, and remote access security, that are needed to qualify for cybersecurity insurance.

Vielen Dank

Bitte kontaktieren Sie uns, falls Sie weitere Fragen haben:
kontakt@beyondtrust.com

beyondtrust.com