Allianz Global Corporate & Specialty SE

CYBERVERSICHERUNG - NEUE TRENDS UND ERFAHRUNGEN

Severin Gettinger

Verband österreichischer Versicherungsmakler, 19.4.2021

Allianz

THEMEN

01 ENTWICKLUNG RISIKO & BEWUSSTSEIN

02 SCHADENERFAHRUNGEN

03 AKTUELLE MARKTHERAUSFORDERUNGEN

TOP 10 GESCHÄFTSRISIKEN WELTWEIT

1 41%

Betriebsunterbrechung
(inkl. Lieferkettenunterbrechung)

2020: 37% (2)

2 40%

Ausbruch einer Pandemie
(z. B. Gesundheits- und Arbeitsschutz, Mobilitätseinschränkungen)

2020: 3% (17)

3 40%

Cybervorfälle
(z.B. Cyberkriminalität, IT-Ausfall, Datenschutzverletzungen, Geldbußen und Strafen)

2020: 39% (1)

4 19%

Marktveränderungen
(z. B. Volatilität, verstärkter Wettbewerb/neue Wettbewerber, M&A, stagnierende Märkte, Marktschwankungen)

2020: 21% (5)

5 19%

Rechtliche Veränderungen
(z.B. Handelskriege und Zölle, Wirtschaftssanktionen, Protektionismus, Brexit, Zerfall der Euro-Zone)

2020: 27% (3)

6 17%

Naturkatastrophen
(z.B. Sturm, Überschwemmung, Erdbeben)

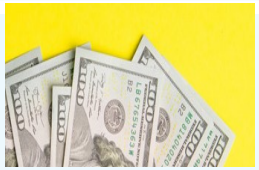
2020: 21% (4)

7 16%

Feuer, Explosion

2020: 20% (6)

8 13%



Makroökonomische Entwicklungen
(z.B. Sparprogramme, Anstieg der Rohstoffpreise, Deflation, Inflation)

2020: 11% (10)

9 13%

Klimawandel/steigende Volatilität des Wetters

2020: 17% (7)

10 11%

Politische Risiken
(z.B. Krieg, Terrorismus, Aufruhr)

2020: 9% (11)

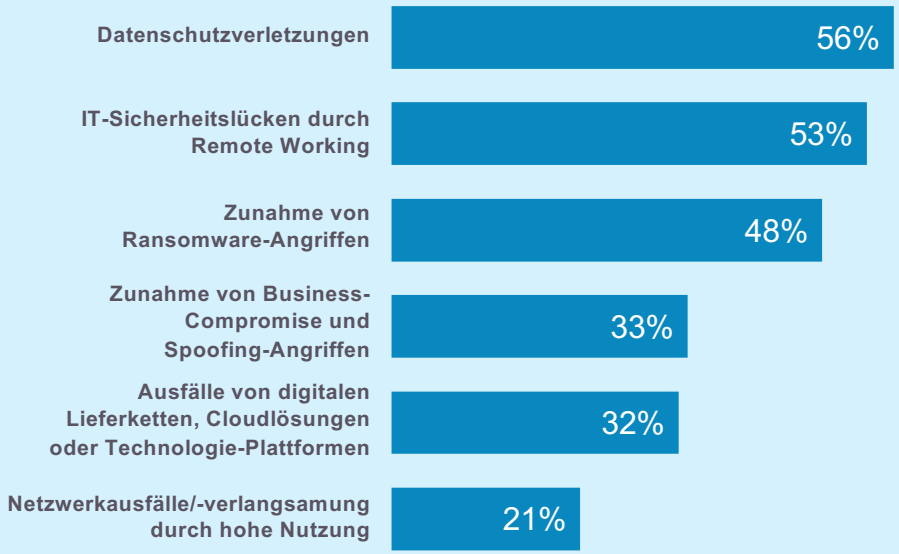
Aufsteiger Absteiger

Quelle: Allianz Global Corporate & Specialty
Die 10. jährliche Umfrage des Allianz Risk Barometers wurde unter Allianz Kunden (globale Unternehmen), Maklern und Branchenverbänden durchgeführt. Außerdem wurden Risikoberater, Underwriter, leitende Angestellte und Schadenexperten im Unternehmensversicherungssegment der Allianz Global Corporate & Specialty und anderer Allianz Gesellschaften befragt. Die Zahlen stellen die Anzahl der ausgewählten Risiken als Prozentsatz aller [illegible] dar. Alle Befragten konnten bis zu drei Risiken pro Branche auswählen, weshalb sich die Zahlen nicht auf 100 % summieren. Aufsteiger sind in rot, Absteiger in grün gekennzeichnet.

CYBER: COVID-19 VERSCHÄRFT IT-SCHWACHSTELLEN

Cybervorfälle:
Vor welchen Cybergefahren sorgt sich Ihr Unternehmen am meisten im Jahr 2021?

Die wichtigsten sechs Antworten

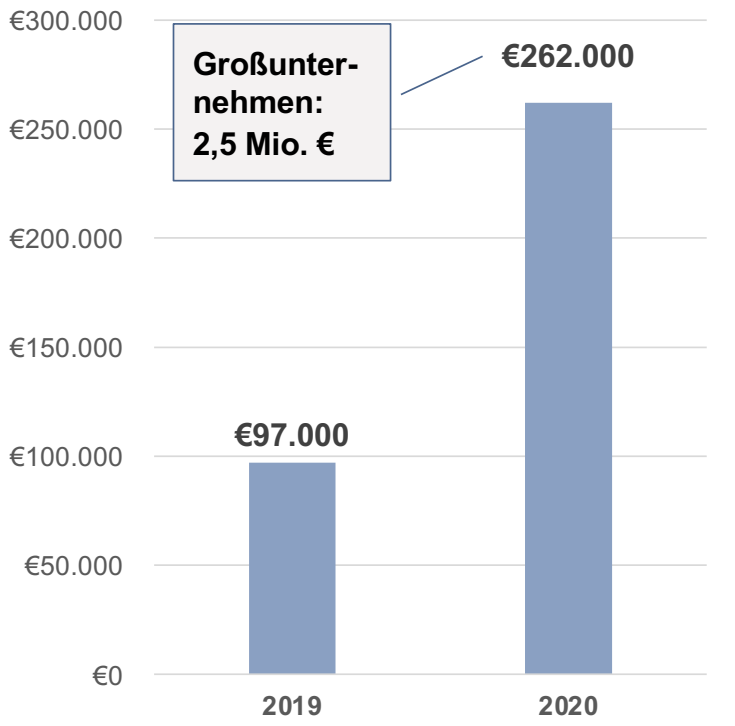


- Covid-19 hat durch die Digitalisierung und Arbeit im Home-Office IT-Schwachstellen weiter verschärft: Covid-19 bezogene Malware- und Ransomware-Vorfälle sind laut FBI und Interpol während Lockdown-Perioden stark gestiegen.
- Ransomware-Angriffe werden immer schädlicher und zielen mit ausgeklügelten Angriffen und hohen Erpressungsforderungen zunehmend auf große Unternehmen.
- Im Jahr 2017 verursachten digitale Angriffe laut Bitkom bei 43% der deutschen Unternehmen Schäden. In 2020 sind es bereits 70%. Die Wahrscheinlichkeit für einen erfolgreichen Angriff liegt bei 45%.

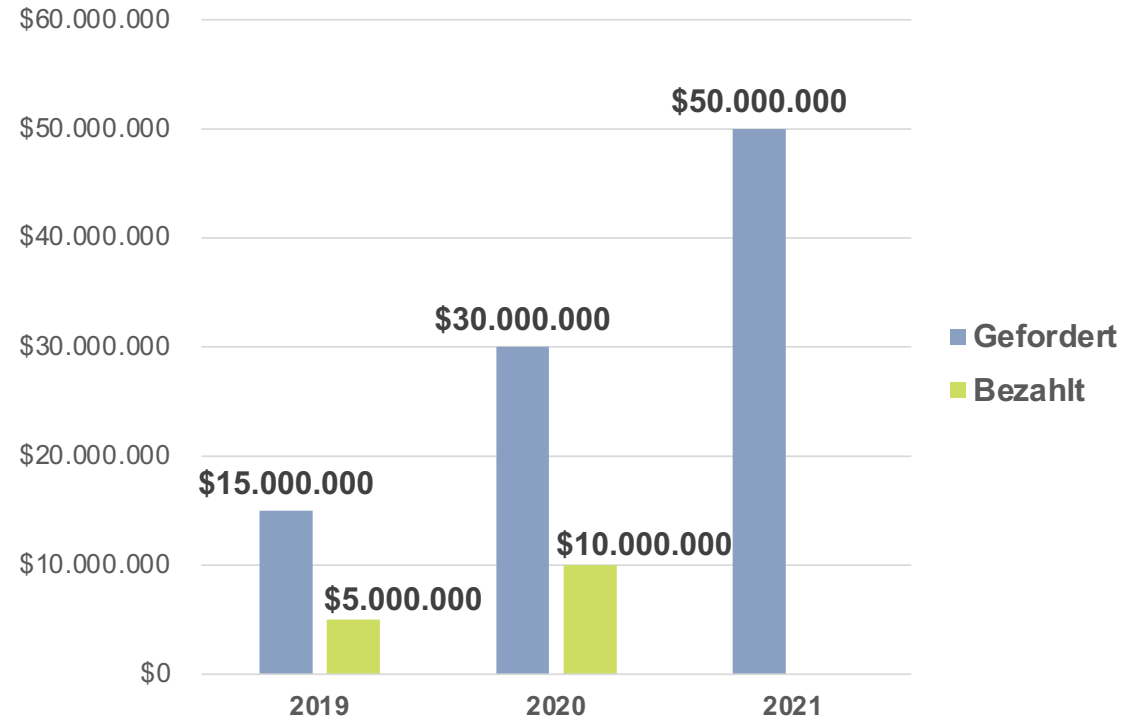
Quelle: Allianz Risk Barometer 2021
Die Prozentangaben beziehen sich auf den Anteil der Umfrageteilnehmer, die diese Frage beantwortet haben: 1.096

LÖSGEGELDFORDERUNGEN & ZAHLUNGEN STEIGEN

Durchschnittliche Lösegeldforderung



Maximale Lösegeldforderung bzw. -zahlung



Quelle: PaloAlto Unit42 Ransomware Threat Report

UNTERNEHMEN NACH WIE VOR NICHT ADÄQUAT AUFGESTELLT

	Erfüllungsquote Kunden 2020
1. Regelmäßige **Trainings** zu Datenschutz und Informationssicherheit	**90%**
2. Sauberes **Patch Management,** inkl. HW/SW Inventar und für EOL Systeme	**~70%**
3. Umfasssende **Backups**, inkl. Wiederherstellung und Separierung	**~80%**
4. Cyber **Incident Response Pläne** existieren und werden getestet	**79%**
5. Ausreichende **Monitoring- and Erkennungsfähigkeiten**	**66%**
6. Multi-Faktor-Authentifizierung für alle Zugriffe von außen	**n.a.**
7. Netzwerksegmentierung für alle kritischen Umgebebungen	**78%**
8. Verschlüsselung der Daten: immer “in transit” und “at rest” wenn sensitiv	**n.a.**
9. Cyber Security Governance, inkl. Verantwortlichkeiten etabliert	**73%**
10. Anti-Malware bzw. Anti-Ransomware Prozesse und Tools im Einsatz	**67%**

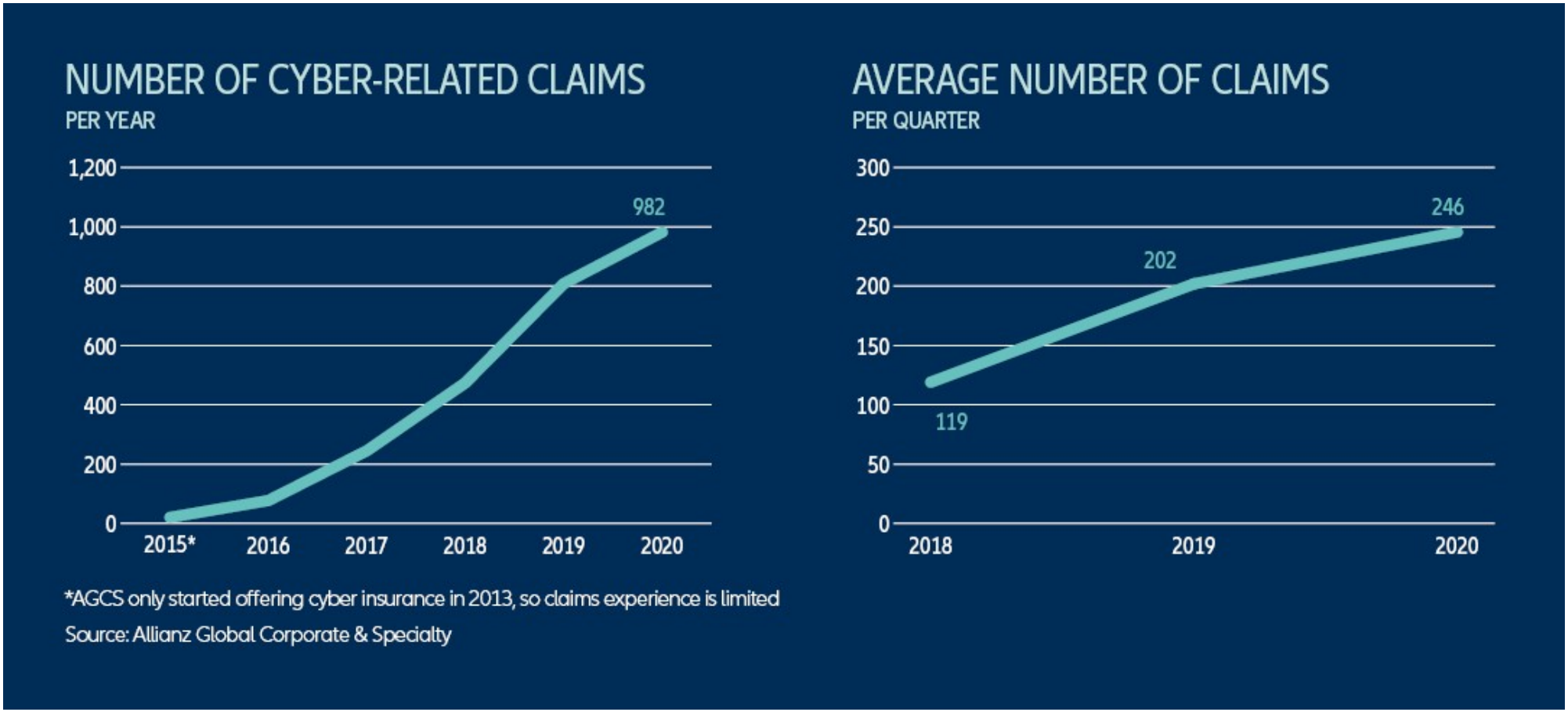
THEMEN

01 ENTWICKLUNG RISIKO & BEWUSSTSEIN

02 SCHADENERFAHRUNGEN

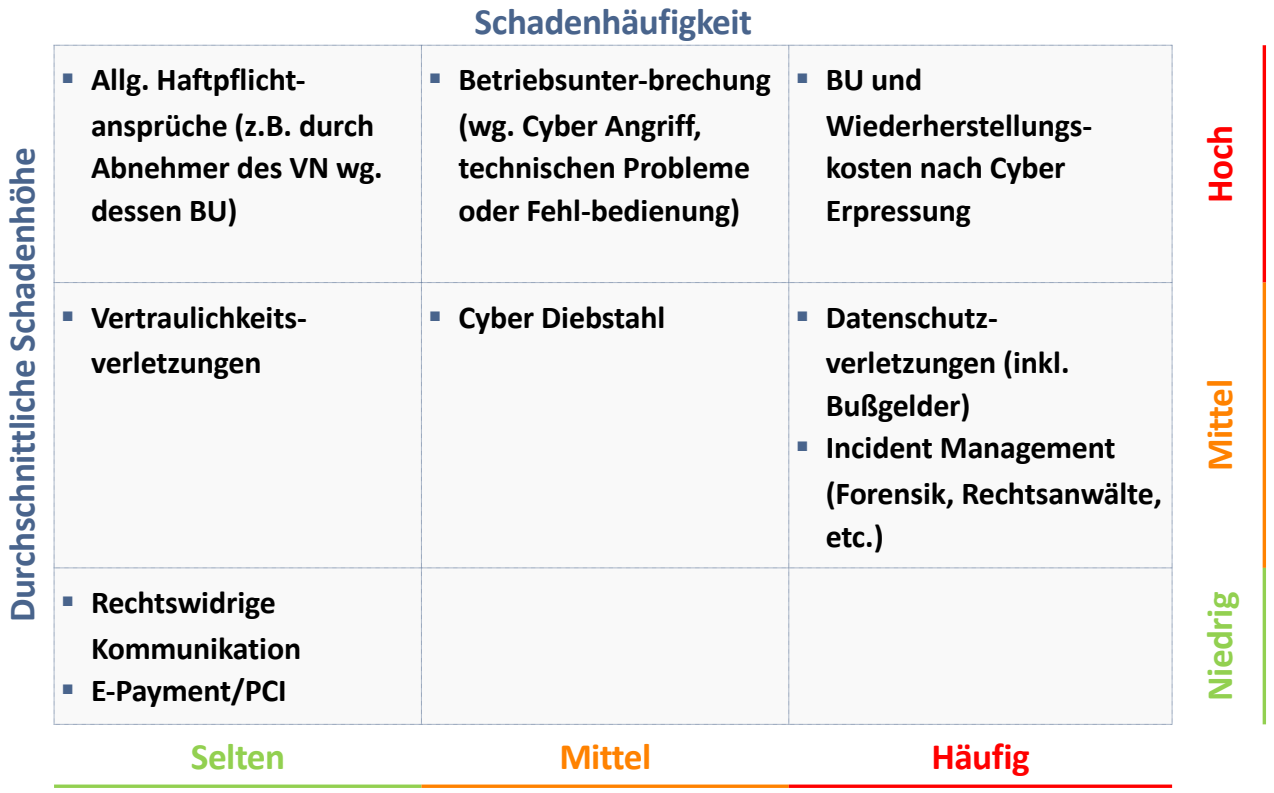
03 AKTUELLE MARKTHERAUSFORDERUNGEN

CYBER SCHADENERFAHRUNG – HÄUFIGKEIT



CYBER SCHADENERFAHRUNG – TRENDS GLOBAL

Gesamtüberblick



Aktuelle Trends

- Ransomware Angriffe häufiger und teurer
- BU nach techn. Problemen tritt verstärkt auf
- Cyber-Diebstahl (nach Cyber Angriff) nimmt zu
- Kosten für IT-Spezialisten bzw. Forensik steigen
- Verhängte Bußgelder nach EU-DSGVO gestiegen
- E-Payment / PCI Schäden selten

CYBER SCHADENERFAHRUNG– FACTS & FIGURES CEE

Quote Verträge mit Schaden/-meldung	~ 25%
Größter Schaden	~ 10 Mio. €
Höchste Quote Schaden/Umsatz eines VN	~ 5%
Höchste Anzahl Schäden und Schaden-meldungen eines Kunden	7
Art von Maßnahmen die den Schaden oft verhindert hätten	Einfachste

Quelle: AGCS Cyber Portfolio CEE

ABGRENZUNG ZU ANDEREN SCHÄDEN

Was decken Cyberversicherungen idR nicht?

- Personenschäden
  - Ausnahme: Persönlichkeitsrechtsverletzungen
- Schäden im Zusammenhang mit Rückruf von Produkten bzw. Dienstleistungen
- Haftpflichtansprüche die nicht auf Cyber-Angriffen beruhen
  - Ausnahme: Ansprüche aufgrund einer Datenschutzverletzung
- Sachschäden, inkl. Vermögensschäden die sich aus Sachschäden herleiten
  - Ausnahme: Schäden an der **IT**-Hardware
- „Gewöhnliche“ Fake President Schäden (ohne Cyber Angriff)

SCHÄDEN UND DEREN VERHINDERUNG

Schadenfälle unserer VN in CEE	Erforderliche Maßnahmen
Computer mit unverschlüsselten Gesundheitsdaten wird gestohlen	Festplatte verschlüsseln (Standard Windows Feature!)
Webserver mit Software aus 2007 wird gehackt (SW-Hersteller längst pleite)	Regelmäßig patchen oder vom Netz nehmen/separieren
Nicht-separiertes Backup wird von Verschlüsselungstrojaner befallen	Zumindest monatlich echtes offline Backup ziehen
Von mehreren Mitarbeitern genutzter eBay Account eines Retailers wird übernommen	Passwort nicht im Team teilen und 2-Faktor-Authentifizierung aktivieren
Komplette Personalliste mit Gehältern, Steuernummern an Externen verschickt	Plausibilitätscheck machen und automatische Anzeige externer Versand
Aufgrund deaktivierten Mailfilters legt Emotet Angriff große Teile des VN lahm	Bereits bestehende Filterung aller ausführbaren Anhänge nicht abschalten

RANSOMWARE AUCH IM KMU-SEGMENT

An
Allianz Vers.AG

[redacted]
Österreich
UP-Code: [redacted]
Tel: [redacted]

[redacted]
Sicherheitsbehörde:

Anzeigebestätigung

über: [redacted] Die komplette Server und EDV Infrastruktur wurde im Frühjahr 2018 auf den neusten technischen Stand gebracht, dh. Server und Clients neu gekauft. [redacted]

Datenbescha

Anzeigeerstattung: Datum/Uhrzeit:
Die Anzeige wird unter oa. Geschäftszahl an StA [redacted]
Schaden entstand durch: Unbekannten Täter

Am heutigen Tage, gegen 06.00 Uhr bekam ich von Frau [redacted] einen Anruf, dass sie in unser EDV System nicht eingesteigen könne (Völlig verschlüsselter Bildschirm) [redacted]

Ca. 50 Minuten später war Herr [redacted] an unserem Standort persönlich vor Ort und hat mich darüber informiert, dass unser System offensichtlich einen massiven Hackerangriff ausgesetzt war. Seit dieser Zeit bemüht sich Herr [redacted] gemeinsam mit einem hinzugekommenen IT Spezialisten der Firma [redacted] unser Betriebssystem wieder in Gang zu setzen. [redacted]

[redacted] auf unserem EDV System eine Mitteilung hinterlegt ist, demnach ein derzeit unbekannter Täter für den Entschlüsselungscode Bitcoins verlangte würde.

[redacted] Jedenfalls ist unser EDV System derzeit blockiert und verliere ich eigentlich stündlich Geld und möglicherweise auch Kunden.

THEMEN

01 ENTWICKLUNG RISIKO & BEWUSSTSEIN

02 SCHADENERFAHRUNGEN

03 AKTUELLE MARKTHERAUSFORDERUNGEN

HERAUSFORDERUNGEN AM CYBER MARKT

Kunden

- In der Breite nach wie vor deutliche Sicherheitslücken
- Awareness steigt, aber Mittel und Personal knapp
- „Kurskorrektur“ bei Angebot

Prämienniveau

- Deutlich unterdurchnittlich im internat. Vergleich
- Schadendaten für aktuarische Prämienberechnung

Angreifer

- Kompetenz und Agressivität wächst (z.B. Double Extortion)
- Hohe Grad Automatisierung Erstangriff

Deckungsumfang

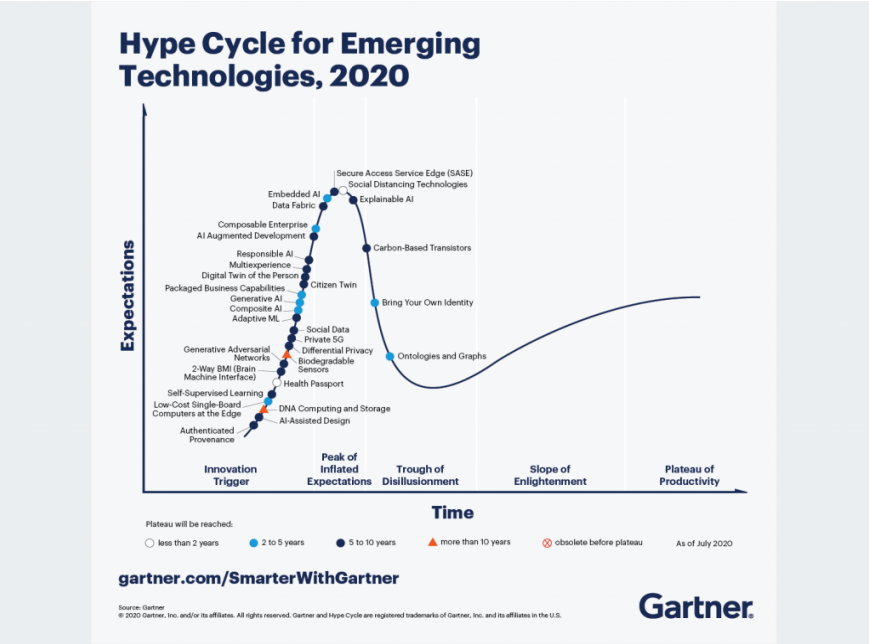
- Breite Deckung bereits in Versicherer-Wordings
- Obliegenheiten / Anforderungen an die VN-IT in den letzten Jahren gesunken

Portfoliomanagement

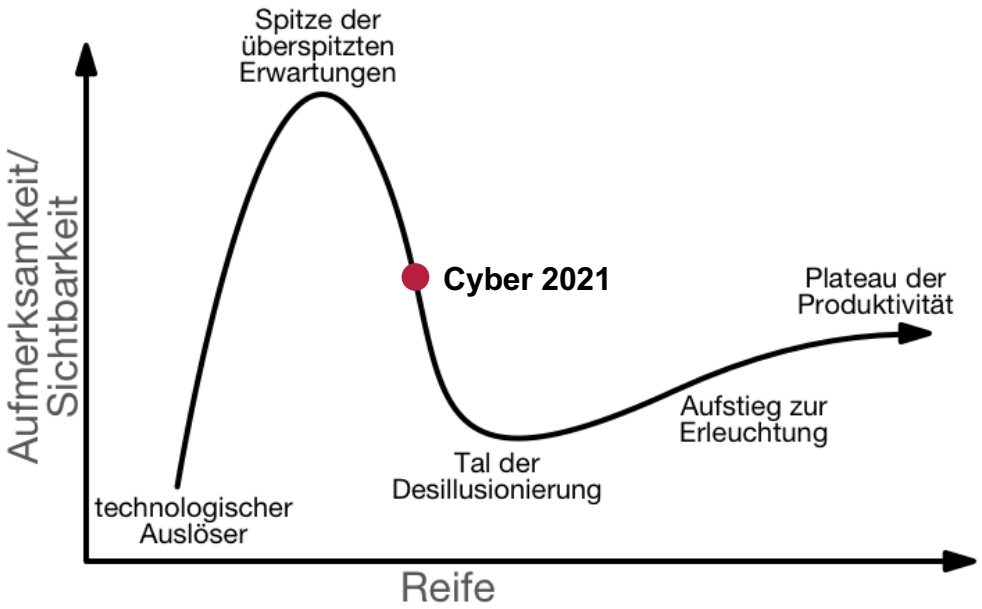
- Begrenzter Markt für Exzedentendeckungen
- Limits hoch im Vergleich zum Gesamtportfolio

TECHNOLOGIE-„HYPE CYCLE“ IN DER CYBERVERSICHERUNG?

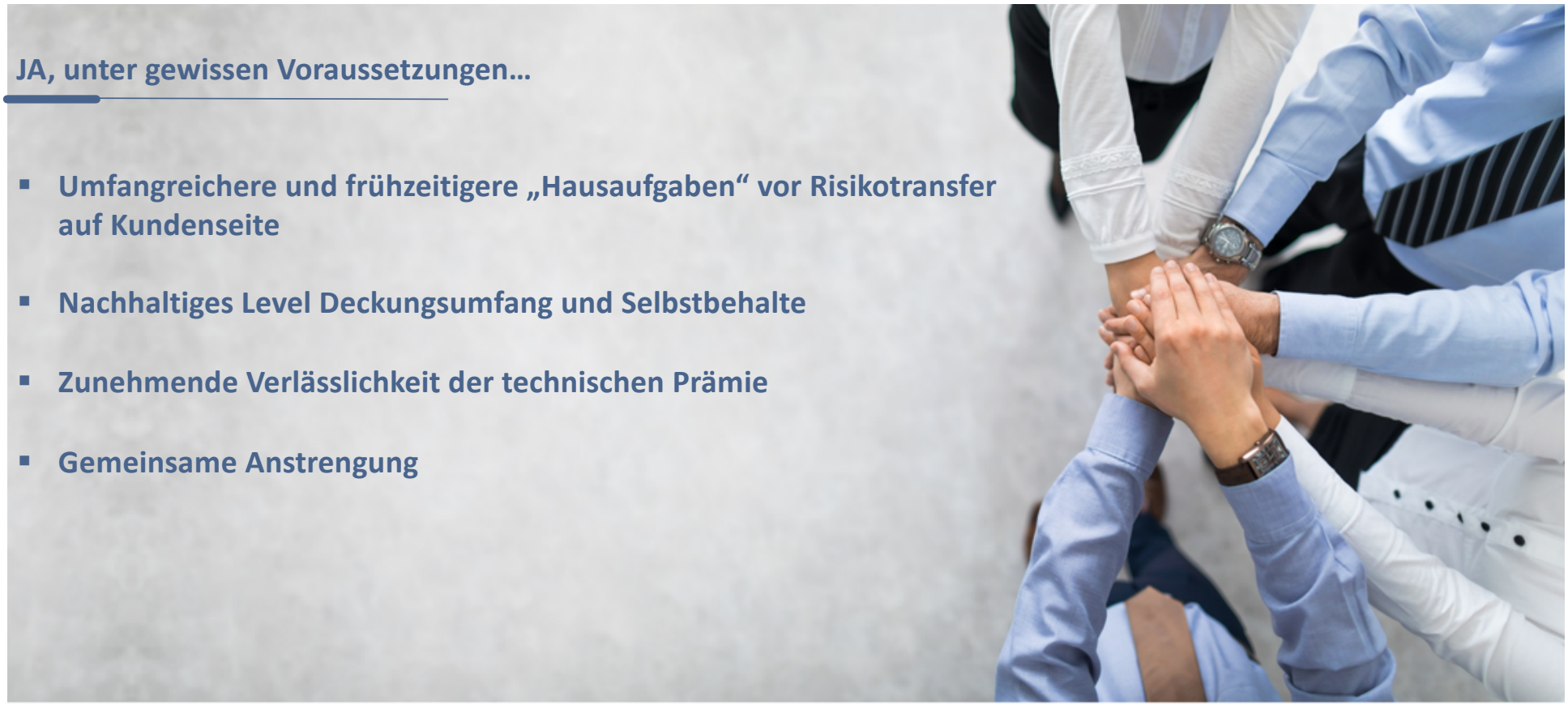
Gartner Hype Cycle Neue Technologien



Status Cyber auf der Reifekurve



BLEIBEN CYBER-RISIKEN VERSICHERBAR?



JA, unter gewissen Voraussetzungen…

- Umfangreichere und frühzeitigere „Hausaufgaben“ vor Risikotransfer auf Kundenseite
- Nachhaltiges Level Deckungsumfang und Selbstbehalte
- Zunehmende Verlässlichkeit der technischen Prämie
- Gemeinsame Anstrengung

DANKE für Ihre Aufmerksamkeit!