Cyber Versicherung: Aktuelle Marktentwicklung und Sicherheitsanforderungen

Michael Winte | Stefan Wolff
15.03.2022

Cyber Versicherung: Marktentwicklung und Sicherheitsanforderungen

Agenda

Zeit		
10.00 – 10.10	**Eröffnung und Begrüßung**	**Michael Winte**
10.10 – 10.25	„Cyber-Versicherung“ Update – aktuelle Marktentwicklung	Michael Winte
10.25 – 11.15	Anforderungen der Versicherer sowie Empfehlungen hinsichtlich der Verbesserung der IT-Sicherheit	Stefan Wolff
11.15 – 11:30	Zusammenfassung und Q&A	Michael Winte Stefan Wolff

Vorbereitung

Mute

Stellen Sie bitte Ihre Mikrophone auf „Mute“

Chat

Für Fragen können Sie jederzeit die Chat Funktion nutzen

Mute

Fragen werden am Ende des Webinars direkt, soweit es möglich ist, beantwortet

Cyber Versicherung: Marktentwicklung und Sicherheitsanforderungen

Agenda

Zeit		
10.00 – 10.10	Eröffnung und Begrüßung	Michael Winte
10.10 – 10.25	**„Cyber-Versicherung“ Update – aktuelle Marktentwicklung**	**Michael Winte**
10.25 – 11.15	Anforderungen der Versicherer sowie Empfehlungen hinsichtlich der Verbesserung der IT-Sicherheit	Stefan Wolff
11.15 – 11:30	Zusammenfassung und Q&A	Michael Winte Stefan Wolff

Cyber Markt 2022

Wo stehen wir und was ist zu erwarten?

Hintergrund Cyberversicherungsmarkt

Die Schadenzahlen steigen weiter, mit einer zunehmenden Zahl kritischer Sicherheitslücken steigt die Angst vor neuen Schadenwellen.

Auch die russische Invasion in der Ukraine geht einher mit einer latenten Cyber-Bedrohung – auch für westliche Unternehmen

In diesem Zuge setzen auch die Versicherer neue Maßstäbe hinsichtlich der Anforderungen an die IT-Sicherheit ihrer Versicherungsnehmer

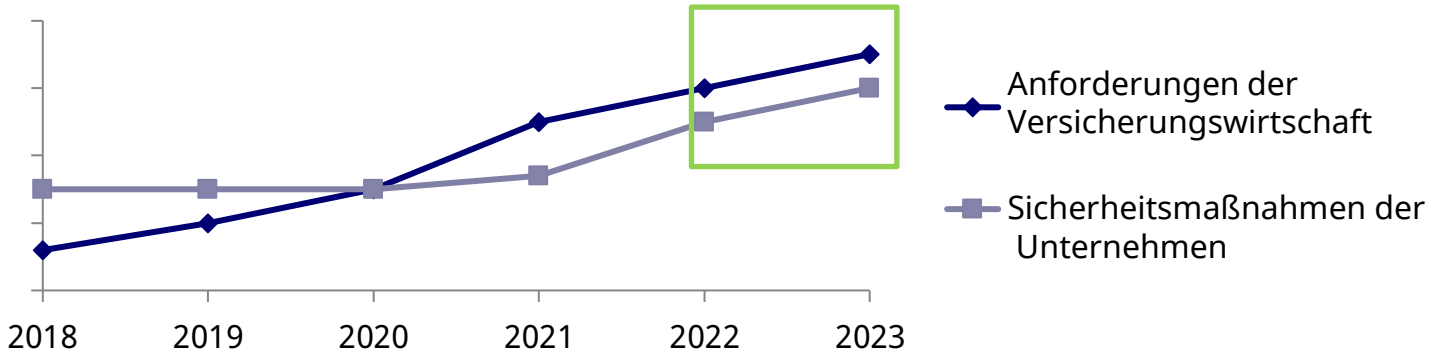
Die zunehmende Vernetzung und Globalisierung sowie regulatorische Anforderungen erschweren die Situation

- Für das kommende Renewal erwarten wir eine weitere Marktverhärtung und steigende Prämien – auch bei schadenfreien Verträgen
- Insbesondere der Umgang mit dem Kriegsausschluss in Cyber-Policen führt am gesamten Markt zu steigender Unsicherheit
- Die Anforderungen variieren je nach Unternehmensgröße – eine Zunahme beobachten wir jedoch für den gesamten Markt
- Insbesondere im Rahmen der Vermarktung und Platzierung von Risiken rücken Risk-Engineering Dienstleistungen immer weiter in den Fokus

Cyber-Markt 2022

Wie ist das Zeichnungsverhalten der Versicherer?

- Seit zwei Jahren verhärtet sich der Cyber-Versicherungsmarkt rapide
- Reduzierung der Versicherungssummen, Erhöhung der Selbstbehalte und Prämien
- Restriktive und massive Anpassungen auch im Renewal
- Weitreichende Underwriting Vorgaben über sämtliche Branchen und Unternehmensgrößen hinweg



Cyber-Markt 2022

Funk Cyber-Team: Wie haben wir uns aufgestellt?

Betreuungsphilosophie der Funk-Gruppe

1	Team: 14-köpfiges Cyber Team in Deutschland | Cyber Hub mit mehr als 30 Personen in der D-A-CH Region
2	Fokus: Cyber Risk Engineering Dienstleistungen › Bestandsaufnahme: Erfassung technischer und organisatorischer IT-Sicherheitsmaßnahmen › GAP-Analyse: Bewertung der IST-Situation anhand der Mindestanforderungen der Versicherer bezogen auf Unternehmensgröße und Branche › Begleitung: Empfehlungen für eventuelle IT-Sicherheitsverbesserungen, ggf. in Kooperation mit ausgewählten Dienstleistern
3	Bedarfseinschätzung: Analyse der individuellen Risikosituation
4	Versicherungsmanagement: Modular gestaltetes Funk-eigenes Bedingungswerk | Beratung | Ausschreibung | Renewal
5	Schadenmanagement: Begleitung des gesamten Prozesses aus technischer und juristischer Sicht

Cyber Versicherung: Marktentwicklung und Sicherheitsanforderungen

Agenda

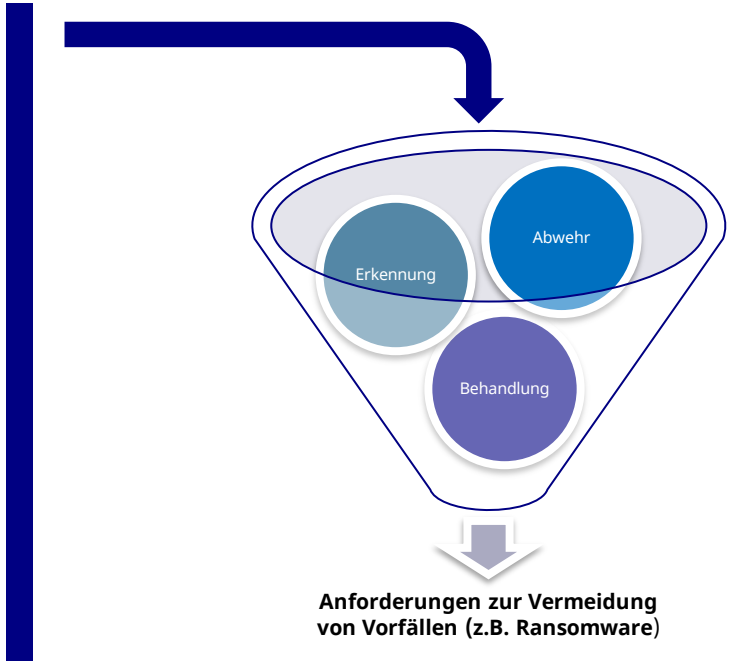
Zeit		
10.00 – 10.10	Eröffnung und Begrüßung	Michael Winte
10.10 – 10.25	„Cyber-Versicherung“ Update – aktuelle Marktentwicklung	Michael Winte
10.25 – 11.15	**Anforderungen der Versicherer sowie Empfehlungen hinsichtlich der Verbesserung der IT-Sicherheit**	**Stefan Wolff**
11.15 – 11:30	Zusammenfassung und Q&A	Michael Winte Stefan Wolff

Analyse & Optimierung der IT-Sicherheit

Was erwarten Versicherer?

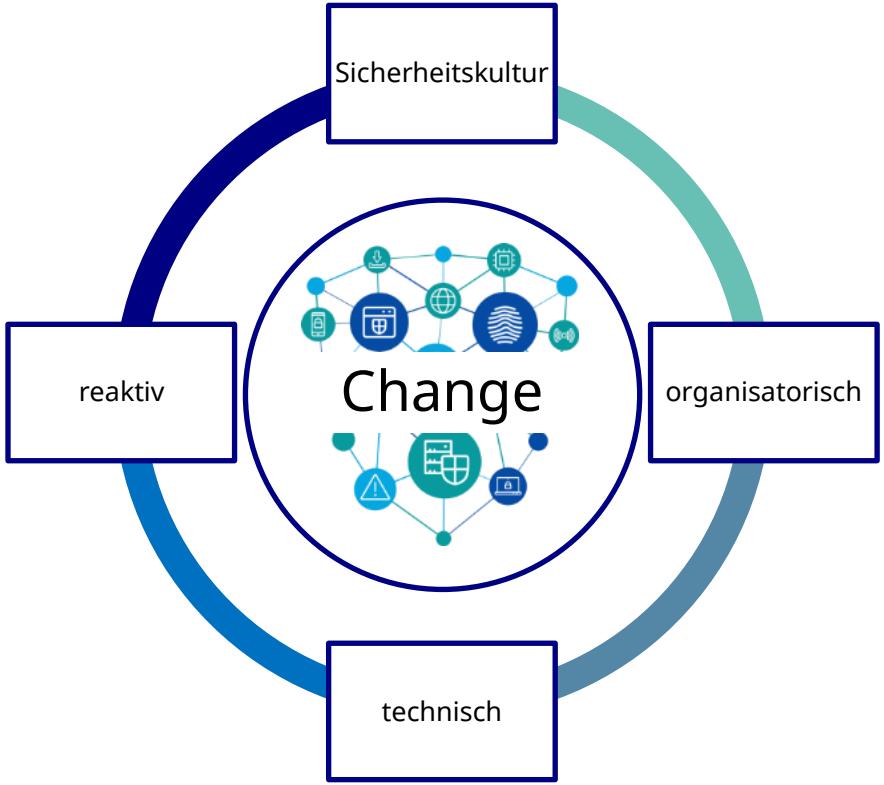
Die Versicherer haben höhere Anforderungen an die Kunden:

1st Line of Defense	Monitoring
Protective Measures	Backup
Recovery	Access Security



Analyse & Optimierung der IT-Sicherheit

Was können Sie tun?



Analyse & Optimierung der IT-Sicherheit

Was können Sie tun?

Sicherheitskultur

1	Angriffe: Frequenz | Intensität
2	Cyber Risiken: Bewusstsein | Auswirkung
3	Arbeitsbedingungen: Anforderungen |Ausbau | Veränderung
4	Digitalisierung: Anwendung | Kontinuität
5	Datenschutz

Analyse & Optimierung der IT-Sicherheit

Was können Sie tun?

organisatorisch

1	Prozesse: Implementierung | Anpassung | Reichweite
2	Richtlinien: Implementierung | Tragweite | Wirkungsgrad
3	Kontrollstrukturen: Ausbau | Verbesserung | Anwendung
4	Monitoring: Anpassung | Verfügbarkeiten
5	Schulungen: DS | IT- / IS | Human Firewall

Analyse & Optimierung der IT-Sicherheit

Was können Sie tun?

technisch

1	Zugriffssicherheit: intern | extern
2	Endpoint Protection: Anforderung | Sichtbarkeit | Reaktion
3	Monitoring: Ausbau | Verbesserung | Anwendung
4	Patch-Management: Frequenz | Situation | Kontrolle
5	Netzwerk: Segmentierung | Absicherung
5	Schwachstellen: Informationen |Ermittlung | Behebung

Analyse & Optimierung der IT-Sicherheit

Was können Sie tun?

reaktiv

1	Datensicherungsmaßnahmen: Backup | Restore | Tests
2	Notfall-Management: Priorisierung |Pläne |Übungen
3	Krisen-Management: Ausbau | Verbesserung | Simulation
4	Kommunikation: intern | extern | Meldeverpflichtung

Analyse & Optimierung der IT-Sicherheit

Fokus der Versicherer

Schwerpunkte 2022

- Zero-Tolerance-Strategie
- Zwingender Einsatz von MFA
- EDR
- Backup-Strategie 3-2-1
- Incident-Response-Planung
- Schwachstellen-Scan
- Monitoring

Anforderungen des Versicherungsmarktes

Kritikalität

Verpflichtende Mindestanforderung aus dem Versicherungsmarkt
Eine Abweichung von dieser Anforderung könnte die Prolongation eines bestehenden Vertrages gefährden und eine Ausschreibung erheblich erschweren oder unwirtschaftlich erscheinen lassen.

Anforderung mehrerer Versicherer und zu erwartende, kommende Mindestanforderung
Eine Abweichung von dieser Anforderung bewerten einige Versicherer kritisch und sie könnte sich negativ auf Ihr Prolongationsangebot oder Ausschreibungen auswirken.

Organisatorisch

Schulungen
Durchführung jährlicher Schulungen zu den Themen der Informationssicherheit (IT- und Datensicherheit sowie Bedrohungen und die eigene Sicherheitsorganisation)

Risikomanagement
Cyberrisiken werden als unternehmerisches Risiko aufgenommen.

Informationssicherheitsmanagement
Es ist ein zentrales und globales Informationssicherheitsmanagement implementiert.

Governance
Das Sicherheitskonzept ist für alle mitversicherten Unternehmen wirksam.

Personal- und Rechte-Management

Review von Benutzerberechtigungen
Benutzerkonten und deren Rechteprofile werden regelmäßig auf Aktualität überprüft und nach Erforderlichkeitsprinzip vergeben.

Schutz sensibler Daten
Zugriffe auf sensible Daten werden ausreichend abgesichert und protokolliert.

Prinzip der geringsten Privilegien
Es wird sichergestellt oder geregelt, dass die Verwendung von Konten mit erweiterten Rechten nur erfolgt, wenn diese benötigt werden.

Passwort-Policy
Es gibt eine verpflichtende Passwortrichtlinie von mindestens acht Zeichen und Komplexitäts-anforderungen ¾. Für privilegierte Konten mit entsprechend höheren Anforderungen.

Zugriffschutz
Zugriffe auf kritische Applikationen werden mittels 2FA/MFA abgesichert.

Schutz privilegierter Accounts
Privilegierte Konten sind in der internen Verwendung mittels 2FA/MFA abgesichert.

Analyse und Optimierung der IT-Sicherheit

Zusammenfassung

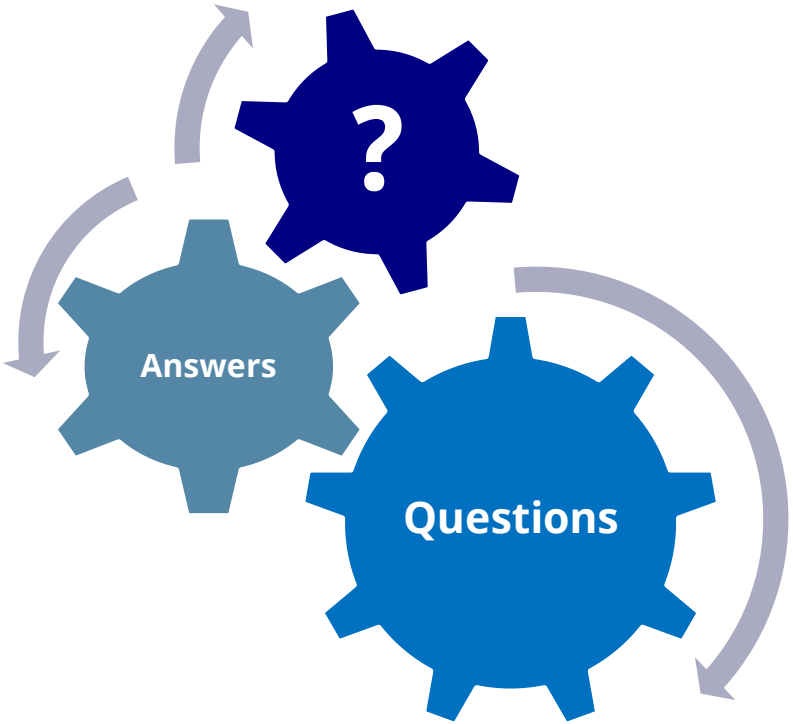
- Ständig steigende Schadenszahlen durch
  - immer schnellere Entwicklung und schlechtere Erkennbarkeit von Malware
  - Professionalisierung von Phishing Angriffen und Varianten
  - Immer häufiger werden neue Schwachstellen durch Zero-Day-Exploits ausgenutzt (Hafnium, Log4J)
  - Angreifer sind hoch organisiert

- Die Anforderungen der Versicherer sind gestiegen
  - Dies bezieht sich auf die Anforderungen an technische und organisatorische Maßnahmen
  - Know-how Bildung und höhere Expertise in der Bewertung von Risiken bei den Versicherern
  - Schadenerfahrung und deren Auswirkungen nehmen massiv zu

- Daraus resultiert für die Versicherungsnehmer
  - technische und organisatorische Maßnahmen sind stetig den veränderten Bedrohungssituationen anzupassen
  - Erkennung, Abwehr und Behandlung sind stetig anzupassen
  - Cyber Bedrohungen sind mit anderen Unternehmensrisiken gleichzusetzen

Cyber-Versicherung: Marktentwicklung und Sicherheitsanforderungen

Q&A



Werte für die Zukunft bewahren
Die beste Empfehlung. Funk.

Wie wir arbeiten: Kundenorientiert – auch bei unseren Medien

Kundenmagazine,
Markt-Spezial, Broschüren

Website mit Themenblog,
Newsletter, Webinare

Podcast, Videos