Aktuelle Marktsituation

Markttrends 2022

Schaden-Kostenquote liegt bei 124%

Cyberversicherer machen erstmals Verluste – Markt legt weiter zu

Hackerangriffe sind eine wachsende Gefahr für die Wirtschaft, zeigen neue Zahlen der Cyberversicherer. 2021 mussten sie deutlich mehr Schäden regulieren, die Aufwendungen überstiegen gar erstmals die Einnahmen. Der Markt wächst indes weiter.

Zuletzt aktualisiert: 13.09.2022 • Lesedauer 6min.

- Starke Marktverhärtung setzt sich fort
- Deutlich verstärkter Fokus der Versicherer auf die Risikosituation der Kunden
  - Qualität der Informationssicherheit von sehr hoher Bedeutung
  - Mindestanforderungen an die IT- und Informationssicherheit
  - Strikte Maßnahmenpläne werden an den Versicherungsschutz gekoppelt

Mindestanforderungen an Unternehmen

Die Mängelliste wird immer länger

- Offline Backup-Lösungen
- Mitarbeiter-awareness Schulungen
- Multifaktor-authentifizierung (MFA)
- Netzwerk-Segmentierung
- Privilegierte Benutzerkonten (PAM)
- Patch-Management
- Endpoint Detection & Response (EDR)

Vorgehen der Versicherer

Fragen über Fragen…

Das Vorgehen ist extrem heterogen

- Angefangen von Fragebögen mit etwa 50 Fragen für KMU
- Über Fragebögen mit 20 Seiten und über 200 Fragen für den Mittelstand
- Bis hin zu ausgedehnten Audits über 3-5 Tage für größere Unternehmen

EIN AUDIT REICHT

Der Risikodialog

ISO Kapitel	Reifegrad
4 Kontext der Organisation	2,75
5 Führung	3
6 Planung	3
7 Unterstützung	2,8
8 Betrieb	3
9 Bewertung der Leistung	2,333333333
10 Verbesserung	2,5
A5 Informationssicherheitsrichtlinien	3
A6 Organisation der Informationssicherheit	3
A7 Personalsicherheit	3
A8 Verwaltung der Werte	2,333333333
A9 Zugangssteuerung	2,75
A10 Kryptographie	3
A11 Physische und umgebungsbezogene Sicherheit	2,5
A12 Betriebssicherheit	2,714285714
A13 Kommunikationssicherheit	3
A14 Anschaffung, Entwicklung und Instandhalten von Systemen	3
A15 Lieferantenbeziehungen	2,5
A16 Handhabung von Informationssicherheitsvorfällen	3
A17 Informationssicherheitsaspekt beim Business Continuity Management	3
A18 Compliance	3

Ausführlicher Report

Aktuelle und qualifizierte Dokumentation über das Informationssicherheitsniveau im Unternehmen samt unterstützende Handlungsempfehlungen vom Experten.

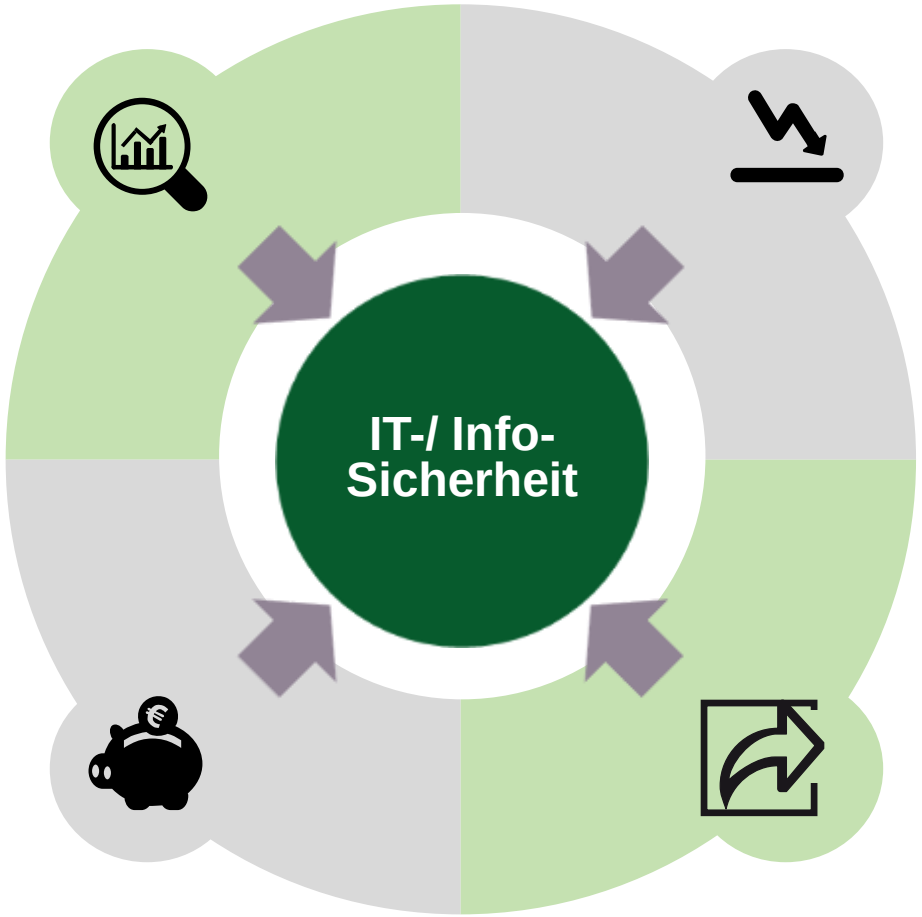
„Deep Dive“

U.a.: Berücksichtigung der aktuellen Schwerpunkte (Painpoints) der Versicherer in Bezug auf die Informationssicherheit und Underwriting.

Umgang mit Cyber-Risiken

Risiken neutralisieren

Risiken reduzieren



Risiken selbst tragen

Risiken transferieren

SCHUNCK CyberComplete Plus

Alles aus einer Hand

24/7 Unterstützung

24/7 – Unterstützung im Krisenfall und in der Informationssicherheit

Deckungskonzept

„State of the Art “ – Bedingungen / Inhalte

Partnernetzwerk

Attraktives Partner-Netzwerk mit Sonderkonditionen

CC CYBER

Ein auf Info-Sicherheit spezialisiertes Competence Center

CYBER-VERSICHERUNG

Fazit & Ausblick – lohnt sich die Investition?

- Wurden die „Hausaufgaben“ gemacht?
  - *Qualifiziertes Risikomanagement?*
  - *Incident Response Prozesse? BCM? ISMS?*

- Cyber-Deckung hat weiter hohe Nachfrage und wird gekauft
  - *Wettbewerbsfähig bleiben / Anforderungen Partner und Kunden*
  - *Mitunter die höchste Prämie in manchen Portfolien der Unternehmen*
  - *Aktuell und vermutlich auch noch länger - „Verkäufer-Markt“*

- Regulierung von Schäden:
  - *Die Regulierungsquote der Versicherer ist hoch*
  - *Obliegenheiten, Vorvertragliche Anzeigepflicht, Fahrlässigkeit*
  - *Interessenskonflikte (u.a.: Intern, mit Dienstleistern, Stakeholdern)*