Cyber-Versicherung: Wann ist ein Unternehmen noch versicherbar?

Dortmund Protected
26.04.2023

Inhaltsübersicht

1. Cyber-Versicherung: Wovor schützt sie?
2. Schadenbeispiele
3. Warum ist Cyber-Versicherung schwierig?
4. Was wird vom Unternehmen gefordert?

1 Wozu?

Unternehmensziel: Informationssicherheit

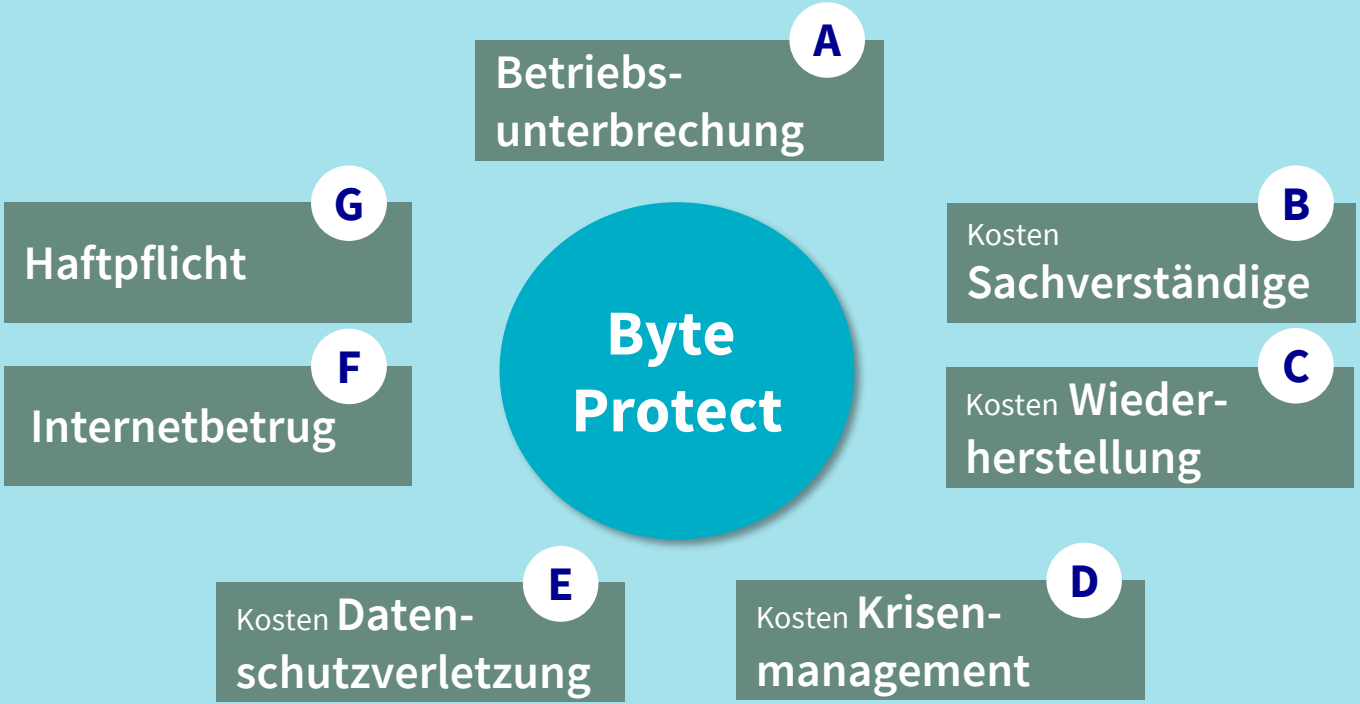
Klären, was geschützt werden soll

- **Geistiges Eigentum**
  Wettbewerbsvorsprung
- **Datenschutz**
  Kundenvertrauen
- **Rechtssicherheit**
  Haftung der Geschäftsführung
- **Kosten reduzieren**
  Schaden verhüten
- **Lieferfähigkeit**
  Verfügbarkeit der Waren

Festlegung

Risikoziele

Bausteine einer Cyber-Versicherung



2 Schadenbeispiele

Schadenbeispiel: Ransomware (I)

Firma:

- Großhandel
- > 500 Mio. Euro Umsatz
- VSU 3 Mio. Euro / SB 25.000 Euro

Schaden:

- Eine Mitarbeiterin in Rumänien klickt auf eine Excel-Datei in einem Mailanhang
- Dadurch Start einer Verschlüsselungssoftware (u.a. ERP und Outlook verschlüsselt)
- Die Attacke wurde über das EDR System erkannt und die verschlüsselten Endgeräte vom Netz genommen
- Backups wohl nicht befallen und werden aufgespielt
- Daher rechnet das Unternehmen damit, morgen wieder in den Normalbetrieb zu kommen.
- **125.500 Euro** für Forensik, Incident Response und Wiederherstellung

Fall

1

Schadenbeispiel: Ransomware (II)

Firma:

- Maschinenbau
- 150 Mio. Euro Umsatz
- VSU 5 Mio. Euro / SB 50.000 Euro

Schaden:

- Ein Quantum Trojaner hat das System befallen
- Der Kunde hat die Verschlüsselung am Morgen bemerkt, sich umgehend abgekapselt und vom Internet getrennt.
- Der „Haus- und-Hof-IT-Dienstleister“ wurde zwecks Forensik beauftragt
- **3 Mio. Euro** für Forensik, Incident Response und Wiederherstellung sowie Betriebsunterbrechung

Fall

2

Schadenbeispiel: E-Mail-Manipulation

Firma:

- Möbelhersteller
- 42 Mio. Euro Umsatz
- VSU 5 Mio. Euro / SB 10.000 Euro

Schaden:

- Die IT stellt fest, dass der Office 365 Account von Herrn D. missbraucht wurde. Jemand (unbekannt) hatte Zugang zum kompletten Account.
- Laut Logs von Microsoft O365 Admin Center jemand aus Lagos/Nigeria.
- Dadurch erhalten zwei Kunden Rechnungen mit einer anderweitigen Kontonummer.
- Die Gelder wurden überwiesen, sind aber nie auf den Konten angekommen.
- Rechnungshöhe: 9.700 US$ und 16.400 US$
- Forensische Untersuchungen durch Microsoft
- **30.000 Euro** für Forensik und Betrugsschaden (in Reserve).

Fall

3

Schadenbeispiel: Lieferketten-Angriff

Firma:

- Stadtwerk
- 500 Mio. Euro Umsatz
- VSU 10 Mio. Euro / SB 100.000 Euro

Schaden:

- Die Firma stellt den Angriff in der Nacht fest
- Nur Office-IT betroffen, keine Netzleittechnik
- Der Angriff erfolgte auf den IT-Dienstleister, nicht auf die Firma direkt
- Dieser IT-Dienstleister betreut auch andere Stadtwerke
- **210.000 Euro** für Forensik und ggf. weitere Kosten (in Reserve)

Fall

4

3 Schwierigkeiten

Warum haben wir ein Problem?

- **Schadensituation**
  in der Cyber-Versicherung nach wie vor dramatisch
- **Ransomware**
  als Haupt-Schadenursache (weiterhin erfolgreich!)
- **Kumulschadenszenarien**
  besonders problematisch (log4j, hybride Kriegsführung, Abhängigkeiten etc.)
- **Sichtbarkeit:**
  Schäden machen Lücken in der Absicherung sichtbar
- **Kenntnis:**
  Es fehlt an Fachwissen bei den beteiligten Parteien

Die Gratwanderung

Bedürfnis der Unternehmen:

- Begleitung auf dem Weg zur Cyber-Sicherheit bei bestehenden Sicherheitsmängeln (Partner in Risk)

Rentabilität der Versicherer:

- Definition der Schwelle zur Versicherbarkeit, um Schadenbelastung spürbar zu senken
- Erkennen von „schlechten“ Risiken

Preise

Bedingungen

Kapazitäten

Risikoselektion

Entwicklung des Risiko-Assessment

Stufe 1

- Wenig Fragen - viele Fragen verhindern Vertriebserfolg
- Keine Obliegenheiten - da im Schadenfall Versicherer stets ablehnen kann (Teufelszeug)
- Wenig technisches Know-how im Underwriting, um Risikoinformationen zu bewerten
- Unsicherheiten, welche normativen Dokumente anzuwenden sind (z. B. Stand der Technik, VdS)

Stufe 2

- Fragebögen explodieren
- Unklar, was Versicherer mit der Vielzahl von Informationen tatsächlich anfangen
- Tarifierungstools, die scheinbare Sicherheit liefern
- Einsatz von Security-Experten bei Risikogesprächen (tlw. externe Firmen)

Stufe 3

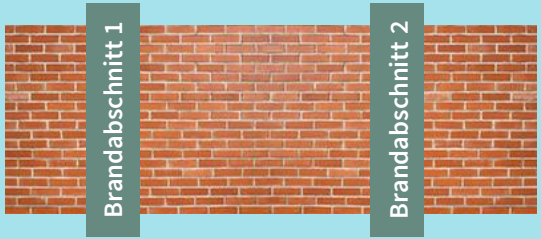
- **?**

Risiko-Assessment – Stufe 3

- **Klarheit über Kernelemente der Absicherung**
  vor wesentlichen Gefahren (Schadenerfahrung)
- **Formulierung von Anforderungen**
  (Transparenz)
- **Die richtigen Fragen richtig stellen**
  (z. B. auf Verständnis des VN abstellen)
- **Die Unternehmen bei der Umsetzung unterstützen**
  (soweit für Versicherer/Makler:in adäquat)
- **Kompetentes Underwriting**
  (Bewertung der Antworten, Formulierung angemessener Auflagen etc.)

4 Anforderungen

Analogie Brandschutz → Cyber-Versicherung



Patch-Management

Firewall

Anti-Viren-Software

Verschlüsselung, Passwortschutz, Berechtigungs-management

Notfallplan

Daten- und Rücksicherung

Präventionskette

Nr.	Was?	Stichworte (nicht abschließend)
1	Schwachstellen von außen erkennen	Schwachstellen-/Port-Scan
2	Mensch / User	Awareness
3	Software-Schwachstellen	Asset-Management - Patchmanagement - kritische Patche - eol-Systeme
4	Lateral Movement	Segmentierung
5	Berechtigungen	Berechtigungsmanagement - Privilegierte Accounts – Fernzugriffe - MFA - MDM
6	Detektion und Reaktion	AV/EDR - NAC - IDS/IPS - Logfiles - SIEM/SOC
7	Backups	Backupkonzept - Schutz vor Manipulation (möglichst offline) - Restore-Tests
8	Vorbereitet sein	Notfallplan - Desaster Recovery - Übungen
9	Ständige Verbesserung	ISMS - Risikomanagement - BCM - Pen-Testing

Risiko-Anforderungen

Beispiel: Backup

Obliegenheit (ByteProtect Rev. 5.1):

Backup: Der Versicherungsnehmer sichert seine betriebskritischen Systeme und Daten risiko-adäquat in angemessenen Abständen (in der Regel werktäglich). Sicherungsdatenträger werden so aufbewahrt, dass sie nicht vom selben Schadenereignis betroffen werden können (in der Regel "Offline-Sicherung").

Fragen:

- Sie sichern Ihre betriebskritischen Systeme und Daten risikoadäquat in angemessenen Abständen (in der Regel werktäglich).
- Es werden mindestens drei Generationen an Sicherungen vorgehalten.
- Sicherungsdatenträger werden so aufbewahrt, dass sie nicht vom selben Schadenereignis betroffen werden können (in der Regel "Offline-Sicherung"). Sofern kein Offline-Backup erfolgt: erläutern Sie, wie sichergestellt ist, dass ein Fremdzugriff nicht möglich ist.
- Es wird regelmäßig (mind. jährlich) geprüft, dass eine Rücksicherung auch tatsächlich möglich ist (Restore-Tests).

Zusätzlich:

Leitfaden Backup, der unsere Anforderungen erläutert und Verweis auf weitere Standards und Arbeitshilfen z. B. von BSI (BSI CON.3)

Weitere Unterstützung

Vorhandene Regelwerke nutzen

- BSI-Grundschutz
- Normen wie ISO 27000 ff, ISIS12 etc.
- Reifegradmodelle wie NIST
- Veröffentlichungen von TeleTrust u.a. zum Stand der Technik

Beratung in Anspruch nehmen

AXA bietet mit dem Partner Swiss IT Security Deutschland GmbH für seine Kunden eine kostenfreie bis zu einstündige Online-Beratung zu Themen der Cyber-Security und Auflagenerfüllung.

Fazit

- Mindestanforderungen an die Cyber-Security sind notwendig
- Diese müssen eindeutig abgefragt und beantwortet werden
- Reifegradmodelle und Zertifizierungen sind hilfreich, aber ohne die harten Kriterien letztlich von geringem Nutzen

Vielen Dank für Ihre Aufmerksamkeit!