Cyber Insurance :

Die Feuerversicherung des 21. Jahrhunderts

(Bild: R adept/CC-BY-SA 4.0)

Mag. Bernhard Ziegler, LL.M.

Versicherungsmakler u. -berater

ZIEGLER

BETRIEBSBERATUNG

Bekannte Fälle

- 2010: Stuxnet und Duqu
- 2014: Hochofen in Deutschland
  (https://www.handelsblatt.com/unternehmen/it-medien/cyberattacke-auf-fabriken-wenn-hacker-den-hochofen-uebernehmen/11138786.html)
- 2015 u. 2018: Deutscher Bundestag
- 2016:
  - FACC : Fake President, Schadenhöhe > EUR 40 Mio.
    - KEIN Cyberschaden im Sinne der Versicherungsbedingungen!
  - LEONI: Fake President, Schadenhöhe EUR 40 Mio.
  - Locky: Ransomware (mehr als 5.000 Infektionen/Stunde)
- 2017: Petya / Not Petya
  - „Most Devastating Cyberattack in History“
    (https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/)
  - „Merck settles $1.4 billion cyberattack case against insurers”
    (https://www.insurancebusinessmag.com/us/news/cyber/merck-settles-1-4-billion-cyberattack-case-against-insurers-471908.aspx)

ZIEGLER
BETRIEBSBERATUNG

Risikofelder im Unternehmen

- Produktion durch Web-/IT-gestützte Systeme
  - Risiko Betriebsunterbrechung/-störung
  - Risiko Fehler in der Produktion
  - Risiko Erpressung
- Transaktionen durch IT-gestützte Systeme (Zahlungsverkehr, Lagerhaltung, etc.)
  - Risiko Verfügbarkeit
  - Risiko Folgeschaden aus Fehltransaktionen
  - Risiko CyberCrime
- Sensible Daten (Zahlungsdaten, Kundendaten, etc.)
  - Risiko Datenschutz-/Vertraulichkeitsverletzungen
  - Risiko Reputationsverlust

Erscheinungsformen

Informationen/Daten werden bedroht

- von außen durch:
  - Hackerangriffe
  - Viren, Malware, Spyware, Trojaner, Würmer (‚Malicious Codes')
  - Spam
  - Social Engineering (Fake President Fraud, Payment Diversion, Phishing, etc.)
  - Kreditkartenbetrug
  - …
- von innen durch:
  - Fehlbedienung und technische Störungen
  - vorsätzliche Schädigungen durch Mitarbeiter:innen
  - veränderte Prozesse (Software-Updates, etc.)
  - …

ZIEGLER
BETRIEBSBERATUNG

Versicherbare Schäden

- Eigenschäden:
  - Rekonstruktion und Wiederherstellung von Daten
  - Betriebsunterbrechung
  - Kosten für die Aufklärung, Forensik
  - Reputationsschäden
  - Erpressungsgelder – strenge Voraussetzungen der FMA
  - unberechtigte Zahlungen (je nach Versicherer)
  - unbrauchbare oder zerstörte Hardware (je nach Versicherer)
- Drittschäden:
  - Schadenersatzansprüche Dritter wegen Vertraulichkeits- und Datenschutzverletzungen, u.a. wegen
    - Datenverluste Dritter
    - Persönlichkeitsrechtsverletzungen
    - Verletzung geistigen Eigentumes
    - Forderungen der Payment-Card-Industrie
  - Vertragsstrafen, Bußgelder (je nach Versicherer)

ZIEGLER
BETRIEBSBERATUNG

Deckung für **Eigen**schäden im Rahmen von

Eigenschäden	SachV	HaftpflichtV	VSV	Cyber
Wiederherstellung Daten u. Programme	teilweise	nein	eingeschränkt	ja
Benachrichtigungskosten gemäß § 24 DSG	nein	nein	nein	ja
BU (fortlaufende Kosten + entgangener Gewinn)	nein	nein	eingeschränkt	ja
Forensik	nein	nein	ja	ja
Krisen-/Reputationsmanagement	nein	nein	ja	ja
Erpressung	nein	nein	nein	teilweise
Computerbetrug	nein	nein	ja	teilweise
Geldbußen	nein	nein	nein	teilweise (soweit gesetzlich zulässig)

ZIEGLER
BETRIEBSBERATUNG

Deckung für **Dritt**schäden im Rahmen von

Drittschäden	SachV	HaftpflichtV	VSV	Cyber
Ansprüche wg. Datenverlust	nein	tw. versicherbar	nein	ja
Ansprüche wg. Datenschutzverletzung	nein	tw. versicherbar	nein	ja
Forderungen der Payment-Card-Industrie	nein	nein	nein	ja
Ansprüche Persönlichkeitsrechtsverletzung	nein	tw. versicherbar	nein	ja
Ansprüche wg. Verletzung geistigen Eigentumes	nein	tw. versicherbar	nein	teilweise
Vertragsstrafen	nein	tw. versicherbar	nein	teilweise

ZIEGLER
BETRIEBSBERATUNG

Beschreibung möglicher Schäden

Schadenszenario	Beschreibung
Betriebsunterbrechung	Sachschadenunabhängige BU (= fortlaufende Kosten, entgangener Gewinn) durch Ausfall der IT oder Datenverlust
Datenwiederherstellung	Mehraufwand zur Wiederherstellung von Daten/Systemen
Forensik	Aufwendungen zur Rekonstruktion einer Timeline des Schadens
Computerbetrug	Datenmanipulation führt zu Fehlüberweisungen
Reputationsschäden	Datenschutzverletzungen schädigen den Ruf des Unternehmens
Datenschutz-/Persönlichkeitsrechtsverletzung	Fehlerhaft programmierte/gewartete Sicherheitssoftware führt zu einem Datenleck
Forderungen der Payment-Card-Industrie	Vertragsstrafen wegen Verletzungen Kreditkartenverarbeitungsvereinbarungen
Verletzung geistigen Eigentumes	Verstöße gegen Urheber-/Markenrechte im Rahmen elektronischer Kommunikation
Benachrichtigungskosten	Nach § 24 Abs 2a DSG bestehen unter gewissen Voraussetzungen Informationspflichten. Zukünftig Verschärfung durch Datenschutzgrundverordnung
Geldbußen	Datenschutzgrundverordnung: Strenge Strafen bei Nichtbeachtung der Informationsverpflichtungen

ZIEGLER
BETRIEBSBERATUNG

Anbieter (Auswahl)

Sicherheitserfordernisse

- Firewall / Virenscanner aktiv
- Verwendung komplexer Passwörter
- Multifaktorauthentifizierung (zumindest bei VPN-Gateways)
- Patch-Management vorhanden
- Wöchentliche Datensicherungen mit Speicherung auf separatem Medium und Überprüfung
- Verwendung von Software, die weiterhin vom Hersteller mit Sicherheitsupdates aktualisiert und aktiv unterstützt wird.
- Regelmäßige Awareness-Schulungen
- Notfallpläne
- Etc.

ZIEGLER
BETRIEBSBERATUNG

Deckungsausschlüsse und Obliegenheiten

- **Korrekte Beantwortung der Risikofragen**
- Gewöhnlicher Verschleiß oder allmähliche Verschlechterung
- Maßnahmen einer öffentlichen oder staatlichen Behörde (zB Beschlagnahme)
- Vorsatz und wissentliche Pflichtverletzungen von Repräsentanten
- Ausfall der Infrastruktur (zB Stromversorgung)
- Terrorismus, Krieg und **Cyber-Operationen**
- Einsatz ungetesteter oder für den Einsatzzweck nicht freigegebener informationsverarbeitender Systeme
- Softwarefehler, welche keine Sicherheitslücke darstellen
- etc.

ZIEGLER
BETRIEBSBERATUNG

Finding Mr. / Ms. Right

- Kein Versicherer bietet alles.
  - dzt. ca. 20 Anbieter am österreichischen Markt
  - relativ wenige Abschlüsse, relativ geringes Prämienvolumen
  - Prämienniveau stabil bis rückläufig
- Probleme
  - Erwartungshaltung
  - Erpressungsgelder
  - Kriegsklausel
- Selbstbehalte
  - betraglich: ab EUR 1.000,-- bis EUR 50.000,-- (und höher)
  - zeitlich bei BU: mindestens 6 / 12 Stunden Wartezeit
- Prämie
  - abhängig vom Umsatz des Unternehmens, Höhe der Versicherungssumme, Selbstbehalte, Sicherheitsniveau etc.

ZIEGLER
BETRIEBSBERATUNG

Alternativen I

Vertrauensschadenversicherung:

Versichert sind durch Vertrauenspersonen verursachte Vermögensschäden, insbesondere wegen

- vorsätzlicher, unerlaubter Handlungen, welche den Schädiger zum Schadenersatz verpflichten (z.B. Betrug, Unterschlagung) oder zur Haftung eines versicherten Unternehmens gegenüber Dritten führen;
- des Verrats eigener oder fremder Betriebs- und Geschäftsgeheimnisse.

Versichert sind auch von Dritten verursachte Vermögensschäden durch

- Raub oder Diebstahl von Bargeld, Wertpapieren oder sonstigen Vermögensgegenständen;
- Täuschung durch Betrug;
- Computermissbrauch (zielgerichtete Hackerschäden)

Probleme:

- Einwand der grob fahrlässigen Herbeiführung des Versicherungsfalles (OLG Frankfurt: zulässig, BGH: ?, OGH: ???)
- KEIN vollwertiger Cyber-Versicherungsschutz

ZIEGLER
BETRIEBSBERATUNG

Alternativen II

Haftpflichtversicherung:

- „Klassische" Betriebs- und Produkthaftpflichtversicherungen bieten mangels Deckung für reine Vermögensschäden bzw. wegen Risikoausschlüssen (zB für Ansprüche wg. Urheberrechtsverletzung) keine ausreichende Deckung.

- Spezielle Vermögensschaden-Haftpflichtversicherungen für IT-Unternehmen bzw. Unternehmen mit Online-Shops sind aber erhältlich.

- Eigenschäden sind aber auch im Rahmen dieser speziellen Haftpflicht-Deckungen zumeist nur sehr eingeschränkt bzw. gar nicht versichert.

ZIEGLER
BETRIEBSBERATUNG