CYBER SCHADENERFAHRUNG – ÜBERBLICK & AUSBLICK

Gesamtüberblick

Durchschnittliche Schadenhöhe

Schadenhäufigkeit

Selten	Mittel	Häufig
▪ Allg. Haftpflicht-ansprüche (z.B. durch Abnehmer des VN wg. dessen BU)	▪ Betriebsunter-brechung (wg. Cyber Angriff, technischen Probleme oder Fehl-bedienung)	
▪ Vertraulichkeits-verletzungen	▪ Cyber Diebstahl	▪ Datenschutz-verletzungen (inkl. Bußgelder) ▪ Incident Management (Forensik, Anwälte, etc.)
▪ Rechtswidrige Kommunikation ▪ E-Payment/PCI		▪ Cyber Erpressungs-zahlungen

Hoch / Mittel / Niedrig

Trends 2018/2019

- Erpressung nach ziel-gerichteten Angriffen häufiger
- BU nach techn. Problemen tritt verstärkt auf
- Cyber-Diebstahl (nach Cyber Angriff) nimmt zu
- Kosten für IT-Spezialisten bzw. Forensik steigen
- Bußgelder nach EU-DSGVO noch nicht erhöht
- E-Payment / PCI Schäden seltener

FALL 1: FEHLÜBERWEISUNG DURCH TÄUSCHUNG NACH CYBER ANGRIFF

*Ein Angreifer schafft es in das Unternehmensnetzwerk des VN einzudringen und **Zugriff auf den Mail-Server** zu erlangen. Somit kann er signierte interne E-Mails versenden und nutzt dies zur **Täuschung einer Finanztransaktion** (Fake President). Das Unternehmen **überweist 6 Mio. €** auf ein ausländ. Konto, welche nach Entdeckung nicht mehr zurückgeholt werden können.*

Ist der Fall gedeckt?

- Besteht Deckung über Cyber? Bedingungsgemäß **Ja (nach Cyber Angriff)!**
- Was ist wenn niemand getäuscht wird (Direkte Überweisung)? **In aller Regel nicht deckungsschädlich!**
- Wie wäre es ohne Cyber Angriff? **Fall für die VSV!**

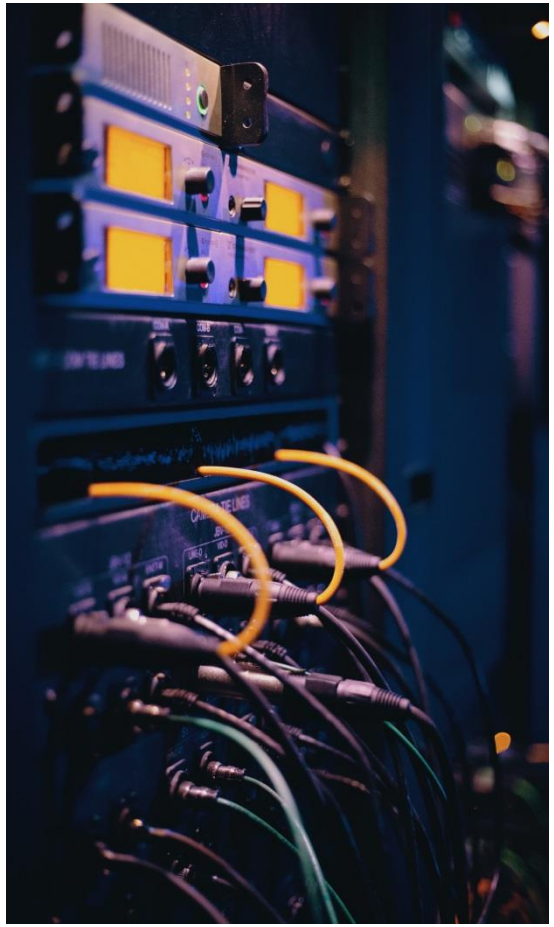
Welche Leistungen würden potenziell fällig?

- Erstattung irrtümlicher Zahlung (ggf. sublimitiert), Forensik, Wiederherstellung, Systemverbesserungen, etc.
- In diesem Fall **keine Leistung** weil noch vor Cyber Vertragsschluss passiert

Source: Pexels.com

FALL 2: BETRIEBSUNTERBRECHUNG NACH TECHNISCHEN PROBLEMEN

*Ein **Hardwaredefekt** in einem Storage Node führt zu Inkonsistenz der zentralen SAP Datenbank. Das **Warenwirtschaftssystem** (alle Einkaufs-, Verkaufs-, Finanz- und Logistikprozesse) **steht für zwei Tage** nicht zur Verfügung. Nutzer können keine An-/Verkäufe tätigen, LKW nicht abgefertigt werden. Nachdem ein **älterer, konsistenter Datenbank-Stand** eingespielt werden muss, sind diverse Nacharbeiten notwendig.*



Ist der Fall gedeckt?

- Besteht Deckung über Cyber? Bedingungsgemäß **Ja (BU nach technischen Problemen)!**
- Greift ein Sublimit? **Normalerweise kein SL vereinbart**

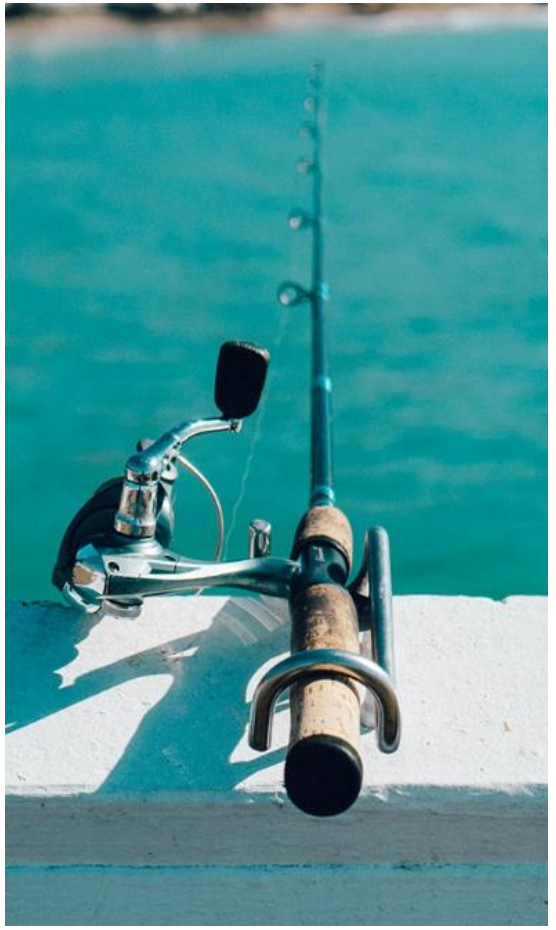
Welche Leistungen würden potenziell fällig?

- Ersatz von **Fixkosten**, insbesondere Gehälter während des Ausfalls
- Erstattung vom **entgangenem Betriebsgewinn**
- **Mehrarbeiten** wie für Inventur, Sonderläufe und manuelle Korrekturen
- Aufwand **Systemwiederherstellung** und **Support durch IT-Dienstleister**

Source: Pexels.com

FALL 3: PHISHING MAIL FÜHRT ZU DATENSCHUTZ-VERLETZUNG UND BETRUG

*Ein Betrüger gibt sich als Vorstand aus und schickt **gefakte Mail** (von außen, kein Cyber Angriff) an HR-Mitarbeiter einer US Tochter unseres VN. Dieser lässt ihm die **Personalstammdaten** (inkl. Social Security Nummern, Steuernummern, etc.) **von ca. 2500 Mitarbeitern** zukommen. Der Angreifer nutzt diese für diverse Betrügereien wie Steuerrückerstattungen. Die betroffenen Mitarbeiter klagen im Rahmen einer Consumer Class Action.*



Ist der Fall gedeckt?

- Deckung bei Datenschutzverletzungen auch ohne Cyber Angriff? ***Ja!***
- Ist (grobe) Fahrlässigkeit bzw. Vorsatz des Mitarbeiters schädlich? ***Nein!***
- Gibt es Deckungseinschränkungen in den USA? ***Nein (bei AGCS)!***

Welche Leistungen werden fällig?

- Rund **USD 1 Mio.** für das Settlement, also Befriedigung der Ansprüche der Mitarbeiter, Credit Monitoring, etc.
- Rund **USD 1 Mio.** für Anwaltskosten
- Schaden somit bei knapp **USD 1.000 pro Datensatz**!

Source: Pexels.com