A · S · P

Assecuranzmakler GmbH

Risiko „Internet“

Die Frage ist nicht „ob“ es einen trifft, sondern

„wann“

A · S · P

Assecuranzmakler GmbH

Schadenbeispiele

Haftpflicht

Durch eigene Unachtsamkeit oder durch Dritte werden vertrauliche Kundendaten „abgegriffen“. Die betroffenen Kunden stellen Schadenersatzansprüche, weil deren Daten missbraucht wurden.

Eigenschäden (kommen **von außen** in das Unternehmen)

- Hackerangriff — Zugriff auf das eigene IT-System über Trojaner, Viren, Würmer, Keylogger, Phishing und Pharming, Scareware, DoS-/ DDoaS-Angriffe

  auf die Webseite des Unternehmens

  - Produkt- oder Preisangaben werden auf der Webseite verfälscht
  - Daten aus Zahlungsvorgängen werden abgegriffen
  - nach Bestellung erhält der Kunde Bestätigungsmails mit geänderten Kontodaten
  - die Webseite wird komplett lahmgelegt

- Schadsoftware — beim Herunterladen von Programmen, Apps, etc. wird das IT-System befallen

- Datenübertragung — infizierte Demoversionen oder Datenträger (USB-Sticks) werden aufgespielt. Anlagen im E-Mailverkehr sind infiziert, werden geöffnet und gelangen so in das System

Erweiterte Eigenschäden (werden **im Unternehmen selbst** verursacht)

- Mitarbeiter — versehentliches, fahrlässiges oder absichtliches löschen von Programmen, Manipulation von Daten, Programme werden falsch aufgespielt, Mails mit sensiblem Inhalt gehen versehentlich an falsche Adressaten, unklare Mailanhänge werden geöffnet, geschenkte USB Sticks werden nicht geprüft, im Internet wird leichtsinnig gesurft, ungeprüfte Freesoftware oder Probeprogramme werden geladen, infizierte Links werden angeklickt, unsichere Passwörter werden benutzt, usw.

- Bedienfehler — bei der Datensicherung- oder deren Rücksicherung

- Datendiebstahl — bewusster Diebstahl oder „Bearbeitung“ von Unternehmensdaten durch Mitarbeiter (z.B. nach Kündigung-/ Versetzung, aus Frust oder Rache am Arbeitgeber)

Betriebsunterbrechung

Durch den Ausfall des IT-Systems können Aufträge weder angenommen, bearbeitet noch abgearbeitet werden. Kundendaten werden manipuliert oder gelöscht. Es entstehen Folgekosten durch

- Betriebsstillstand
- Ausweichen auf andere Bereiche / Betriebe
- Lieferverzug
- Annahmestopp
- Behelfseinrichtungen

Vertragsstrafen

Wenn die Vereinbarungen mit dem Betreiber des Zahlungssystems zur Kreditkartenbenutzung (Payment Card Industry Data Security Standard) verletzt werden.

[weitere Infos unter „Schadenbeispiele“]

A · S · P

Assecuranzmakler GmbH

Die Schlüsselfrage: „wie lange kann ohne Zugriff auf das eigene Netzwerk gearbeitet werden“

- ohne Kunden — und Adressdaten, Kontakte zu Zulieferern und Abnehmern, Terminvorgänge, Mailkontakte, Archivierte Dokumente, sensible oder persönliche Daten wie Analysen, Geschäftsberichte, Bilanzen, Gesundheits- oder Finanzdaten
- ohne Bank — zu laufenden oder terminierten Zahlungsvorgängen, Kontozugänge, Passwörter, Kreditkartenzahlungen, usw.
- ohne Programme — eigene Anwenderprogramme, Buchhaltungssoftware, spezielle und hochkomplexe Programme für die voll- oder teilautomatische Steuerung von Maschinen (CNC Maschinen, Fließbandfertigung, Massenproduktion, etc.)
- ohne Internet — eigene Webseite, Webshop-/ Onlineverkauf

Mindestanforderungen und Checkliste an die eigene IT-Sicherheit

- eine permanente Datensicherung - unabdingbar, zzgl. den Tests zur Wiederherstellung der Daten
- ein Systemadministrator - fasst unverzichtbar
- sichere und wechselnde Passwörter
- Schulung und Sensibilisierung der Mitarbeiter z.B. beim Surfen im Internet und beim E-Mailverkehr
- unterschiedliche Benutzerhierarchien (für Administrator- und Benutzer)
- aktuelle Firewall, Virenscanner, laufende Updates, Backups, usw.
- 2-Faktor Authentifizierung (bei Online-Bankgeschäften)

A · S · P

Assecuranzmakler GmbH

Was sollte in einer Cyberpolice enthalten sein

Wie wird geholfen?

- 7 Tage die Woche / rund um die Uhr
- per Telefon, durch spezialisierte IT-Experten
- per Fernwartung, durch Aufschaltung auf das eigene Netzwerk
- vor Ort, wenn „nichts mehr geht“

A · S · P

Assecuranzmakler GmbH

Welche Kosten sind über eine Cyberpolice gedeckt

(**Auszug !**)

- die Kosten eines behördlichen Ermittlungsverfahrens wegen angeblicher Datenrechtsverletzung, wegen des Vorwurfes der Verletzung von Persönlichkeits-, Urheber-, Marken- oder Wettbewerbsrechten
- für gesetzliche oder behördliche Benachrichtigungspflichten (wenn z.B. eigene Kunden über den Hackerangriff informiert werden müssen)
- eigene Anwaltskosten
- die Kosten für eine Rechtsschutzdeckung, wenn das Unternehmen selbst Unterlassungs- und Widerrufsklagen einleitet
- Kosten qualifizierter Dienstleister zur Erstanalyse des befallenen Netzwerkes
- Kosten zur Einleitung erster Gegenmaßnahmen
- die Kosten von Spezialfirmen, welche die EDV nach einem Angriff „säubern“ und Sicherheitsstandards wieder herstellen (bestenfalls mit dem eigenen Firmen-Administrator oder der angebundenen IT-Firma)
- Kosten externer Dienstleister, wenn diese nach einem Cyberangriff mit der eigenen Datenüberwachung beauftragt werden. (Überwachung des IT-Systems für einen Zeitraum von bspw. 12 Monaten)
- Kosten der Wiederherstellung von Daten und Programmen
- Aufwendungen für die eigene Reputation
- Vertragsstrafen für Unternehmen, welche am elektronischen Karten-/ Zahlungsverkehr teilnehmen und vom Betreiber des Zahlungssystems in Anspruch genommen werden
- fortlaufende Kosten und entgangener Gewinn bei Betriebsunterbrechung wegen eines Softwareschadens
- Schäden aus Erpressung, Bedrohung, Betrug (Manipulation von Webseiten, z.B. Identitätsdiebstahl)
- Mehrkosten, weil Daten nicht mehr zur Verfügung stehen
- die Webseite Offline oder das Internet ausgefallen ist
- Ausfallkosten durch externe IT Dienstleister (Cloud Dienste)
- für die Abwehr von Erpressungen (Hacker verschlüsseln das Computersystem und verlangen Geld)
- für die Krisenberatung während einer Erpressung
- Kosten aus Onlinebetrug durch Phishing, Pharming

Phishing	das Stehlen von persönlichen Daten mittels gefälschter E-Mails und Webseiten
Pharming	die Weiterleitung auf gefälschte Webseiten durch manipulierte Browser

A · S · P

Assecuranzmakler GmbH

Was kostet das

Unternehmen mit Umsätzen bis 10 Mio. €

- Prämienberechnung nach Umsatz des Unternehmens
- einfaches „Antragsmodell“ (übersichtlich und einfach aufgebaut)
- Deckungsumfang analog zu Industriebetrieben
- umfangreiche Assistance Dienstleistungen inkl. Cyber-Hotline
- Deckungssummen von **100.000 €** bis **2.500.000 €**
- Selbstbehalte [SB] von **1.000 €** bis **5.000 €**
- Jahresbeiträge ab **300 €**
- Kurzfragebogen mit wenigen und einfachen Risikofragen
- direkter Versicherungsschutz und sofortige Policierung

[für Unternehmen **ab 10 Mio. €** Umsatz erfolgt eine individuelle Risikobewertung und Prämiengestaltung]

Prämienbeispiele (Stand 2022)

Umsatz : bis 250.000 €
Deckungssumme : **250.000 €**
SB : 1.000 €
Jahresnettoprämie : **460 €**

- Bedienfehler, Betriebsunterbrechung durch Cloud-Ausfall, Über-/ Unterspannung, Geldbußen nach DSGVO sind bis jeweils **20.000 €** mitversichert

Umsatz : bis 1.000.000 €
Deckungssumme : **500.000 €**
SB : 1.000 €
Jahresnettoprämie : **820 €**

- Bedienfehler, Betriebsunterbrechung durch Cloud-Ausfall, Über-/ Unterspannung, Geldbußen nach DSGVO sind bis jeweils **30.000 €** mitversichert

Umsatz : bis 5.000.000 €
Deckungssumme : **2.000.000 €**
SB : 1.000 €
Jahresnettoprämie : **2.435 €**

- Bedienfehler, Betriebsunterbrechung durch Cloud-Ausfall, Über-/ Unterspannung, Geldbußen nach DSGVO sind bis jeweils **120.000 €** mitversichert

➢ Individuelle Erhöhung der Sublimits generell möglich