CYBERCRIME
DIE TÄGLICHE REALITÄT!

Haben Sie schon vorgesorgt?

VERSICHERUNGEN

DR. SCHMITT VERSICHERUNGSMAKLER

EIN UNTERNEHMEN DER BANK SCHILLING

Foto: Glebstock/Fotolia

CYBER: IT-Risiken in einer neuen Dimension – Ransomware auf dem Vormarsch

Häufigkeit und Schweregrad der Cyberschäden steigen vehement. Risikomanager in Unternehmen sind immer stärker darin gefordert, Cyberrisiken kalkulierbar zu machen.

Nahezu sämtliche unternehmerischen Aktivitäten sind heute abhängig vom Austausch elektronischer Daten über interne und externe Datenleitungen – Tendenz steigend. Kriminelle und Unbefugte sind jederzeit in der Lage, sich in fremde IT-Systeme einzuschleusen und dort großen Schaden zu stiften.

Risiken im Cyberraum bedrohen jedes Unternehmen

Als Unternehmer sollten Sie sich über eines im Klaren sein: unzureichender Cyberschutz ist und bleibt folgenschwer:

- Cyber – Haftung
  Schadenersatzansprüche Dritter wegen Sicherheitsverletzungen im Cyberraum, z.B. fehlgeschlagene Abwehr eines Hackerangriffes

  Die Cyber-Haftpflicht-Versicherung übernimmt:

  - die Prüfung des Anspruches
  - die Abwehr unberechtigter Ansprüche
  - die Befriedigung berechtigter Ansprüche

- Cyber – Eigenschaden
  Kosten und Verlust von Einnahmen, z.B. Wiederherstellungs- und Rekonstruktionskosten bei Verlust oder Beschädigung von Daten und Programmen, entgehende Einnahmen bei Betriebsunterbrechung durch einen IT-Systemausfall oder Verlust von Daten, Erpressungsgelder

- Zusätzliche Kosten
  Unfreundliche Begleitp(k)osten im Schadenfall, z.B. für Krisenmanagement, PR-Berater oder Buß- und Strafgelder bei einem Datenschutzvorfall

Internetkriminalität steht nach wie vor hoch im Negativ-Kurs, jedoch ist erst jedes zehnte Industrieunternehmen entsprechend versichert. Die Schadenzahl für alle offiziell angezeigten Fälle 2015 in der BRD beträgt laut BKA 40,5 Mio. EUR. Bitcom schätzt die Höhe weitaus höher, sogar auf 22,4 Mrd. EUR pro Jahr. 60 Prozent aller registrierten Attacken wurden dabei von sogenannten Insidern verübt, die Folgen wiegen damit doppelt schwer für Industrie und Wirtschaft.

Ransomware ist und bleibt auf dem Vormarsch

Einer Umfrage zum Thema Ransomware (Schadprogramme) zufolge ist mit 75 Prozent die Infektion aufgrund arglosen Umgangs mit infizierten E-Mail-Anhängen die häufigste Ursache. Technologie allein schützt noch niemanden, somit bleibt das Restrisiko Mensch. Ein einziger, unbedachter Klick eines Mitarbeiters reicht aus, um ein komplettes Unternehmen lahmzulegen. Daher ist neben technischen Maßnahmen die Schulung der Mitarbeiter zusammen mit einem übergreifenden Backup-Konzept unabdingbar.

Das amerikanische FBI berichtet beispielsweise über einen dramatischen Anstieg von Fällen, in denen Betrug über vorgebliche Geschäftsführungsanweisungen begangen wird (CEO Fraud). Bei dieser Betrugsmethode werden E-Mails an Mitarbeiter verschickt, die Nachrichten des Managements vortäuschen, um Geldüberweisungen auszulösen.

Prävention gegen nicht zielgerichtete Attacken

Hinzukommend sind sich viele leider nicht bewusst, dass bisherige Versicherungspolicen eine eingeschränkte Absicherung beinhalten und überwiegend nur dann greifen, wenn der Angriff eine spezielle Absicht hat und nicht ziellos vonstatten geht. Das Problem: Zahlreiche Cyberangriffe sind nicht auf bestimmte Ziele gerichtet. Hacker streuen ihre Viren oft wahllos und warten darauf, dass diese an

CYBER: Sorgen Sie vor – Gute Gründe für eine Cyberversicherung

irgendeiner Stelle eindringen können – gleichgültig wo, jedoch meist mit Erfolg und verheerenden Schäden.

Wir berücksichtigen bei unseren Versicherungsprodukten beide Formen des Angriffs und können Sie bestens beraten, für einen optimalen Cyberschutz.

Gute Gründe für Ihre Cyberversicherung

- Daten sind eines Ihrer wichtigsten Güter, jedoch über konventionelle Versicherungen nicht oder nur teilweise versichert.

- Reibungslos funktionierende IT-Systeme sind für das tägliche Gelingen Ihrer Geschäfte unverzichtbar. Über traditionelle Betriebsunterbrechungsversicherungen sind Unterbrechungen aufgrund von Cyberangriffen jedoch nicht gedeckt.

- Cybercrime ist die weltweit am schnellsten wachsende Verbrechenssparte.

- Daten und Informationen werden immer wertvoller und für den Verlust fremder Daten kann Ihr Unternehmen zur Verantwortung gezogen werden. Bei Verlust von Kreditkartendaten drohen Händlern harte Strafen.

- Image ist das Kapital Ihres Unternehmens – Sie sollten es versichern. Unbefugter Zugriff auf Ihre Social Media Accounts oder der Verlust sensibler Kundendaten kann Ihrer Reputation erheblich schaden.

- Portable Laufwerke vervielfältigen die Gefahr von Verlust oder gar Diebstahl. Zunehmende Nutzung von Smartphones und die Verwendung von Cloud-Anwendungen im Unternehmen bieten eine weitere Angriffsfläche für Kriminelle im Cyberraum.

Versicherbare Schadenpositionen

- Schadenersatzansprüche Dritter
- Abwehr unberechtigter Ansprüche
- Ausgleich berechtigter Ansprüche
- Ertragsausfall infolge einer Betriebsunterbrechung
- Kosten für forensische Untersuchungen
- Kosten für Rechtsberatung und PR-Berater
- Wiederherstellungskosten bei Verlust bzw. Zerstörung eigener Daten und Netzwerke
- Erpressungsforderungen durch Hacker
- Benachrichtigungskosten bei Verstößen gegen Datenschutzvorschriften

Gewiss bestehen eines oder mehrere Risiken auch bei Ihnen – sprechen Sie uns einfach an. Wir unterstützen Sie bei Ermittlung, Bewertung und Transfer betrieblicher Risiken auch dieser Art.

Technik und Recht, Risiken und Versicherungslösungen verändern sich mit großer Geschwindigkeit: Wir halten für Sie Schritt – und Ihr Risikomanagement auf dem neuesten Stand.

Mit freundlicher Unterstützung der Erichsen GmbH, www.erichsengmbh.de

Dr. Schmitt GmbH Würzburg
- Versicherungsmakler -
Dieselstraße 2 – 6 | 97082 Würzburg
Telefon 0931 45075-0
Telefax 0931 45075-555
E-Mail: kontakt@dsv-wzbg.de
www.dsv-wzbg.de

VERSICHERUNGEN
DR. SCHMITT VERSICHERUNGSMAKLER
EIN UNTERNEHMEN DER BANK SCHILLING