

POOLWORLD

Fachmagazin für Finanzdienstleister

IM AGE WECH SEL DICH

Wie junge Talente
den Maklerberuf
neu definieren

Alle unter einem Dach
Ein exklusives Hausverwalter-
konzept macht Schluss
mit dem Verwaltungschaos

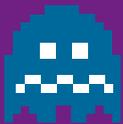
Von der Pflicht zur Chance
Ein kritischer Blick auf zwei
Jahre ESG-Beratungspflicht
in der Praxis

Die bAV zahlt sich aus
Immer mehr bAV-Verträge kommen
in die Auszahlung. Wir sagen,
worauf es dabei ankommt



Digitalen Fortschritt in Unternehmen erkennen und richtig versichern

Digitalisierung. Ein großer, umfassender Begriff, der uns allen fast täglich begegnet. Vorgänge aller Art werden so beschleunigt, komprimiert und zentralisiert. Es ist uns möglich, in Sekundenschnelle mit Menschen auf der ganzen Welt zu kommunizieren und Vorgänge weltweit zu vernetzen. Effizient, ökonomisch und ökologisch, das sind wohl die drei Grundideen der Digitalisierung und einer vernetzten, digitalen Welt.



Doch neben den vielen Vorteilen, die die Digitalisierung uns bringt, entstehen neue Gefahren und Sicherheitslücken, die versichert sein müssen. Eine Sensibilisierung für jene Risiken soll dieser Artikel bewirken, wenngleich das Thema viel umfassender ist, als wir es uns heute vorstellen können.

Jedes Unternehmen arbeitet mit sensiblen Daten, seien es Namen und (Mail-)Adressen, Kontodaten oder Telefonnummern. Diese Daten werden meist zentral und verschlüsselt gespeichert auf einem Server oder in einer Cloud. Also unerreichbar für Hacker? Nein! Unzählige Tricks, von der einfachen Phishing-Mail über den Trojaner bis hin zu groß angelegten, gezielten Hackerangriffen, existieren in unserer digitalen Welt.

Vor allem Vermögens- und Reputationsschäden können die Folge solcher Cyberangriffe sein. Die damit verbundenen Datenwiederherstellungskosten können schnell in ungeahnte Höhen steigen. Zumal das Bundesdatenschutzgesetz den Unternehmen dort auch Strenge im Schadenfall auferlegt.

1. BEISPIEL :

Die Sekretärin eines Immobilienmaklerunternehmens fällt auf eine Mail herein, die täuschend echt wirkt und angeblich vom Inhaber höchstpersönlich kommt. Darin bittet er um die Tätigkeit einer Überweisung von 30.000 Euro auf ein Konto, welches angeblich einem Geschäftspartner gehört. Selbst eine Bevollmächtigung für jene Transaktion ist der Mail beigefügt und beinhaltet die beiden Unterschriften der Geschäftsführer. Die Sekretärin tätigt die Überweisung und das Geld ist verloren.

2. Beispiel:

Hacker greifen die IT eines Hotels an und stehlen durch einen „Infostealer-Trojaner“ sämtliche Kreditkarteninformationen der Hotelgäste. Daraus entstehen unter anderem Kosten für die Datenwiederherstellung, die Forensik und für den eventuellen Austausch der Kreditkarten durch die Hersteller.



Henry Falkenberg,
Fachberater Sach- und Gewerbeversicherung



Die Cyberversicherung schützt adäquat vor den Vermögensschäden, die durch die Gefahren des Internets entstehen können; beispielsweise Kosten für die Rechtsberatung, Forensik sowie für Kreditüberwachungsleistungen und die Betriebsunterbrechung.

Aber nicht nur klassische Datensätze können gestohlen, sondern beispielsweise auch Maschinen gehackt werden. Die künstliche Intelligenz (KI) ist immer mehr auf dem Vormarsch und nimmt uns schon heute viele Arbeiten ab. Roboter und autonome Systeme sind in der Lage, komplexe Aufgaben auszuführen, zum Beispiel in einer Tischlerwerkstatt. Werden solche Systeme gehackt, können schnell existenzbedrohende Vermögensschäden entstehen. Zum einen der Ertragsausfall, zum anderen auch die Reparatur der Maschinen oder die Kosten aus einer möglichen Gesamtverzögerung in der Lieferkette.



3. BEISPIEL:

KI-gesteuerte Maschinen in einer Werkstatt werden durch einen Verschlüsselungstrojaner gehackt und stillgelegt. Die Hacker verlangen für die Wiederinbetriebnahme ein horrendes Lösegeld. Dem Inhaber der Werkstatt bleibt keine Wahl, als das Lösegeld zu zahlen. Zusätzlich entstehen Kosten durch die Betriebsunterbrechung und für die neue Installierung sowie Konfigurierung der Systeme und Maschinen.

Alle daraus entstehenden Kosten, die sich auf mehrere Hunderttausend Euro beziffern können, sind über eine Cyberversicherung gedeckt. Vertriebliche Zielgruppen für eine Cyberversicherung sind praktisch alle Unternehmen, die im täglichen Geschäft viel mit IT respektive KI zu tun haben. Das kann ein kleines oder mittelständisches Hotel sein, digitalisierte Handwerksbetriebe, Handels- und Dienstleistungsunternehmen oder auch Logistikbetriebe, deren Abläufe zumeist stark digitalisiert sind.

Zu guter Letzt noch eine Empfehlung, wo das Cyberrisiko gut versichert ist. Hier wissen primär die Markel und die Hiscox mit starken Leistungen zu überzeugen. Dort haben versicherte Unternehmen eine 24h-Hotline, eine Mitversicherung ungezielter Angriffe, aber auch einen Versicherungsschutz ohne die Einschränkungen hinsichtlich Arten von Cyberangriffen oder der genutzten Schadsoftware. Die Hiscox ersetzt darüber hinaus Belohnungsgelder für Hinweise auf kriminelle Aktivitäten, wenn jene zur erfolgreichen strafrechtlichen Verfolgung eines Beteiligten führen. Zuzüglich sind die Kosten für das Krisenmanagement abgedeckt, heißt zum Beispiel für dessen Aufbau und Ausrüstung.

Die voranschreitende Digitalisierung eröffnet Unternehmen nicht nur neue Chancen, sondern konfrontiert sie auch mit neuen Risiken, die existenzbedrohend sein können. Wenn selbst ausgereifte IT-Sicherheitskonzepte scheitern, schützt die Cyberversicherung vor den daraus resultierenden Vermögensschäden. Sprechen Sie Ihre Gewerbekunden aktiv auf dieses wichtige Thema an – unsere Komposit-Abteilung unterstützt Sie gern dabei. ◀

Kontakt:

Team Komposit-Management
040 29 99 40-390
komposit@maxpool.de

