

Datum 04.10.2017

VSV versus Cyber – welche Absicherung benötigt mein Kunde?

Kennen Sie den Unterschied zwischen Vertrauensschaden und Cyber?

Eine Cyber-Versicherung hätte Payment-Diversion-Fraud oder den Fake-President nicht gedeckt! Warum?

Cyber-Deckungen ersetzen häufig **Eigenschäden** sowie **Schäden bei Dritten**, beispielsweise bei Vertragspartnern und Kunden, die durch Hacker-Angriffe, DoS-Attacken (Denial of Service engl. für Dienstverweigerung), Computermisbrauch, Diebstahl von Datenträgern oder eine sonstige Datenrechtsverletzung auftreten. Insbesondere sind die Übernahme der Kosten für professionelle Ersthilfe im Schadensfall durch die Vermittlung von IT-Spezialisten und Fachanwälten, Schadenermittlung, Public-Relations-Maßnahmen und Rechtsverfolgung häufig Teil des Leistungsumfangs.



Täuschungen und Betrug der Buchhaltung durch Dritte – auch über das Internet – sind jedoch in der Regel nicht umfasst.

Beim **Fake-President-Betrug** nehmen die Täter Kontakt zu Mitarbeitern eines Unternehmens auf (über die sozialen Medien, E-Mail oder Telefon). Dabei geben Sie sich beispielsweise als Geschäftsführer, leitender Angestellter oder Handelspartner des Unternehmens aus. Ziel der Kontaktaufnahme ist der Transfer eines Geldbetrages ins Ausland.

Ein neuer Betrugs-Trick hat es auf die Zahlungsströme zwischen Geschäftspartnern, mit denen man in der Regel schon seit Jahren zusammenarbeitet, abgesehen. Der **Payment Diversion Fraud**, zu Deutsch das Umleiten von Zahlungsströmen, startet im Prinzip wie der Fake-President-Betrug mit einem Social-Engineering-Angriff. Die Betrüger geben sich in diesen Fällen als **Geschäftspartner oder Lieferanten** des Unternehmens aus und erreichen durch gefälschte Mitteilungen, dass die Bezahlung für Waren oder erbrachte Dienstleistungen auf abweichende Konten erfolgt. Die Umsetzung dieser Form des Betruges wird ermöglicht durch eine gefälschte Information an das Unternehmen, dass sich die bisher vereinbarten Bankverbindungen geändert haben und der Zahlungsverkehr nun über die **neue Bankverbindung** abgewickelt werden soll. Viele Geschädigte merken dies erst, wenn sie Zahlungsaufforderungen von diesem Lieferanten erhalten. **Opfer sind häufig KMU**. Die Betrugssummen liegen im fünf- und sechsstelligen Bereich.

Versicherungsschutz bei Payment-Diversion oder dem Fake-President-Betrug bietet die **R+V-VermögensschutzPolizze bei Internet- und Wirtschaftskriminalität!**

Kontaktieren Sie uns gerne unter kredit@ruv.at für ein individuelles Angebot, oder verwenden Sie unseren Tarifrechner (www.tarifrechner-ruv.at).

Unser Einführungswebinar zur R+V-VermögensschutzPolizze können Sie sich [hier ansehen](#).

Ansprechpartner: Herr Christian Narten, Underwriter Kredit + Kaution

Die Informationen in diesem Newsletter sind sorgfältig geprüft worden. Trotz aller Sorgfalt können sich aber Angaben zwischenzeitlich verändern. Eine Haftung oder Garantie für die Aktualität, Richtigkeit und Vollständigkeit der zur Verfügung gestellten Informationen kann daher nicht übernommen werden. Gleiches gilt auch für alle Websites, auf die mittels eines Hyperlinks verwiesen wird. Für den Inhalt der Websites, die mit einer solchen Verbindung erreicht werden, sind die oben genannten Anbieter nicht verantwortlich.

Impressum

Herausgeber dieses Newsletters:

R+V Allgemeine Versicherung AG
Niederlassung Österreich - Hauptbevollmächtigter: Dkfm. Dr. Martin Beste
Sitz: Wilhelmstraße 68, 1120 Wien
Firmenbuch: HG Wien Fn 351083z, UID-Nr. ATU 65994944, DVR 4003621
Hauptsitz: R+V Allgemeine Versicherung Aktiengesellschaft, Raiffeisenplatz 1, D-65189 Wiesbaden
Handelsregister Nr. HRB 2188, Amtsgericht Wiesbaden, USt-IdNr. DE 811198334

Verantwortlich für den Newsletter:

Dominic Gantner
Leitung Marketing & Vertriebssupport

Redaktion:

Telefon: +43 1 810 5333 0
E-Mail: makler@ruv.at