Cyber-Interview mit den Kolleginnen aus der Schadenabteilung.

Nicole Gustiné, Verkaufsförderung Firmen/Freie Berufe
Meike Löchelt, Leiterin Betriebshaftpflicht/Transport Schaden
Britta Kruse, Schadenaufsicht Firmen/Freie Berufe

NG: *Hallo Frau Löchelt, Cyber ist in aller Munde und gleichzeitig gibt es immer wieder Fragen zum Schadenprozess. Was sollte ein Versicherungsnehmer, wenn er etwas Ungewöhnliches feststellt, als Erstes tun?*

ML: *Der Versicherungsnehmer sollte umgehend unsere Schaden-Hotline* **0511 3031-562** *anrufen und am besten für die Meldung des Schadens die Versicherungsnummer seiner Cyber-Police sowie Kontaktdaten für Rückfragen unseres IT-Sicherheitsdienstleisters bereithalten. Weitere wichtige Anweisungen finden Sie auch in unserer Schadenbroschüre inkl. Einlegeblatt, dort ist das richtige Verhalten im Schadenfall detailliert beschrieben.*

NG: *Wir werden oft gefragt, warum der Versicherungsnehmer nicht direkt bei unserem IT-Sicherheitsdienstleister anrufen soll, sondern bei der HDI Cyberschaden-Hotline?*

ML: *Der IT-Sicherheitsdienstleister deckt einen Ausschnitt unserer Deckung ab, d. h. insbesondere die Schadenfeststellung und -abwehr und die Forensik. Mit der HDI Cyberversicherung Stand-alone unterstützen wir aber im Fall der Fälle auch bei der Auswahl eines geeigneten Rechtsanwalts mit der Expertise IT-Sicherheit und Datenschutz, einer geeigneten PR-Agentur, die Sie bei der Krisenkommunikation unterstützt, bei der Auswahl eines Dienstleisters zur Überwachung von Kreditkarten oder Fachleuten zur Datenrettung und Schadeneindämmung. Daher ist es so wichtig, dass die Strippen bei uns zusammenlaufen und wir immer als Erstes informiert werden, um bedarfsgerecht zu koordinieren.*

NG: *Für allgemeine Rückfragen zum Produkt haben wir ein Postfach eingerichtet: Cyberversicherung@hdi.de. Trotzdem höre ich immer wieder, dass Kolleg(inn)en bei Fragen zum Produkt die HDI Cyberschaden-Hotline anrufen, können Sie auch hier weiterhelfen?*

ML: *Nein! Diese Nummer ist ausschließlich für unsere Kunden im Schadenfall reserviert! Alle anderen Fragen können wir nicht beantworten und die Kolleg(inn)en werden blockiert, sodass es im Schadenfall zu Kapazitätsengpässen kommen könnte.*

NG: *Frau Kruse, warum soll der Kunde sich bei dem Verdacht eines Cyberangriffs eigentlich sofort melden und nicht erst genauer prüfen, welches Problem er hat?*

BK: *Durch eine sofortige Meldung kann der Angriff bestenfalls umgehend abgewehrt und der Schaden eingedämmt werden. Sofern kein Versicherungsfall vorliegt, wird die Forensik und Schadenfeststellung innerhalb von 48 Stunden ohne Anrechnung des Selbstbehalts durchgeführt.*

NG: *SEC Consult bietet auch einen Kurz-Check der Sicherheitsstandards vor Vertragsbeginn an. Wie funktioniert der Erstkontakt?*

BK: *Für den Kurz-Check zu den Sicherheitsstandards sendet der Kunde einfach eine Mail an: hdi-security-check@sec-consult.com. Ein Mitglied des Incident Response Teams von SEC Consult wird ihn dann umgehend kontaktieren, um ihm ein Angebot zukommen zu lassen, und nach Einwilligung bzw. Unterschrift dann auch umgehend mit den Überprüfungen anfangen. Beim Nichtbestehen eines Checks wird der Kunde mit einem standardisierten Maßnahmenkatalog für den besagten Kritikpunkt versorgt. Die Maßnahmen kann er dann entweder selbst oder durch einen IT-Dienstleister umsetzen lassen.*

NG: *Was beinhaltet der Kurz-Check?*

BK: *Der Kurz-Check beinhaltet einzelne Module, die separat gebucht werden können. Zudem bieten wir einen Paketpreis, wenn alle Sicherheitsstandards überprüft werden sollen.*

NG: *Wir bekommen hinsichtlich der Berufsgruppe Steuerberater immer wieder Rückfragen zur Datenauslagerung in eine Cloud wie z. B. DATEV. Wir haben hierzu eine umfangreiche Information erstellt. Aus dem Vertrieb wurde uns jetzt ein aktueller Schaden geschildert, der sich genau mit dieser Thematik beschäftigt, können Sie uns dazu etwas berichten?*

BK:/ML: *Ja, sehr gerne. Ein Steuerberater, der im Jahr rund 30.000 Euro an die DATEV bezahlt, ist gehackt worden. Es wurden 15 Arbeitsplätze lahmgelegt inklusive Back-ups auf seinem Server. Es gab auch die Bitte, 5 Bitcoins zu überweisen.*

Die Kanzleien arbeiten häufig auf zwei Ebenen online, bei der DATEV ist sicherlich eine gute Sicherung vorhanden und Daten können wiederhergestellt werden. Was aber, wenn die Mitarbeiter die DATEV-Arbeitsebene verlassen, weil sie ins Internet gehen, in Outlook Mails mit Anhängen öffnen usw.? Eine Kanzlei hat ja auch weitere sensible Daten, wie Personaldaten o. Ä. Alleine die Wiederherstellung des Systems dauerte drei Wochen, wovon die Mitarbeiter eine Woche zu Hause bleiben mussten – also auch das Thema Betriebsunterbrechung wurde aktuell. All das wäre mit einer Cyberversicherung gedeckt gewesen!

NG: *Frau Löchelt, Frau Kruse, vielen Dank für Ihre Zeit und die ausführlichen Informationen.*

HDI Vertriebs AG
30659 Hannover
www.hdi.de/cyberversicherung

7003041171-201810