CYBER-RISK-VERSICHERUNG

Gerade kleine und mittelständische Firmen sind von den neuen digitalen Risiken nicht ausgenommen. Eine offizielle Studie des internationalen Konzerns KPMG bestätigt, dass trotz gestiegener Sensibilität 38 % aller deutschen Unternehmen in den vergangenen 2 Jahren bereits angegriffen wurden (siehe „E-crime in der deutschen Wirtschaft 2017“, KPMG AG, 2017). Hier geht es zur e-crime-Studie (PDF)

Die Frequenz der Cyber-Angriffe wird in Zukunft voraussichtlich weiter ansteigen. Ein hohes Risiko haben vor allem Unternehmen, die sensible Kundendaten in ihren Systemen speichern und ihre Prozesse oder ihre Produktion hauptsächlich digital steuern. Somit gehören neben dem produzierenden Gewerbe beispielsweise auch Krankenhäuser, Ärzte, Logistikunternehmen, Online-Shops oder Versicherungsberater/-makler zu den potentiellen Zielen für eine Cyberattacke. Die Konsequenz ist häufig eine hohe finanzielle Belastung mit teilweise existenzbedrohendem Ausmaß. Antivirensoftware und Firewall bieten zwar einen physischen Schutz, doch häufig reicht dieser nicht aus, um sich vor einem Cyberangriff erfolgreich zu schützen.

BCA TIPP

Hier geht es zum globalen Cyberkrieg: http://map.norsecorp.com/#/
Die Karte der Hackerangriffe von der IT-Sicherheitsfirma Norse ist nett visualisiert, sollte allerdings nicht zu ernst genommen werden. Quelle: dpa-tmn/tsn

Hotline: Tel.: (0 61 71) 91 50–180, Fax: (0 61 71) 91 50–181, E-Mail: gewerbe@bca.de
BCA AG, Frankfurter Landstraße 62 a, 61440 Oberursel, www.bca.de

Welche Gefahren können ein Unternehmen treffen?

Datenmissbrauch Über Schadsoftware, gestohlener Hardware oder auch ausgeliehene Zugänge werden Daten ausspioniert. Bank- und Kreditkartendaten-Klau gehört zu den häufigsten Missbräuchen, da hier viel Geld gemacht werden kann.

Datensabotage Schadprogramme löschen, beschädigen oder verändern Daten beim Kunden.

Erpressung Über Schadprogramme (Trojaner) werden Rechner des Kunden stillgelegt. Nur wenn der Kunde ein Lösegeld zahlt wird die Blockade aufgehoben. Oft werden auch Daten entwendet und dann mit Veröffentlichung gedroht. Gerade sensible Personen-, Gesundheits-, Bank- und Kreditkartendaten können ein Druckmittel sein.

Mailbomben Gezieltes Versenden von einer Vielzahl an E-Mails um den Empfänger zu blockieren.

DoS-Attacke (Denial of Service). Hier spricht man von einer Dienstverweigerung, die im Internet zur Beeinträchtigung von Webservices führt, und die, als DoS-Attacke ausgeführt, einen angegriffenen Server oder eine Website außer Betrieb setzen kann.

Welche Kunden sind potenzielle Ziele?

Krankenhäuser, Ärzte, das produzierende Gewerbe, Logistikunternehmen, Online-Shops, Onlinehandel mit Zahlungsabwicklung und -dienstleistung oder Inkassodienstleistung und die Versicherungsbranche inkl. Vermögensverwaltungen, Banken bis hin zum Versicherungsmakler.

Welche Kosten und Leistungen wären versicherbar?

Vertrauensschäden, Rechtsberatungen, Kosten für Wiederherstellung, IT-Forensik, PR-Beratung, Krisenmanagement und Informationen, Zahlungsmittelschäden, Lösegeldzahlungen, anfallende Vertragsstrafen, Kreditüberwachungsdienstleistungen, Betriebsunterbrechungsschäden, Sicherheitsverbesserungen, Cyber- und Daten-Eigenschäden und die Cyber-Haftpflicht.

Welche Sicherheitsvorschriften werden von den Versicherern verlangt?

Durchgängiger Virenschutz mit aktuellen Virensignaturen, Firewallstrukuren an allen Netzübergängen zu externen Netzen, abgestuftes Rechtekonzept mit administrativen Kennungen ausschließlich für IT-Verantwortliche, regelmäßige (mindestens tägliche) Datensicherung auf separierten Systemen oder Datenträgern, Der Antragsteller führt regelmäßige (mindestens tägliche) Datensicherungen auf separierten Systemen oder Datenträgern durch. Der Antragsteller nutzt eine Anti-Virus-Software und eine Firewall für seine stationären IT-Systeme. Diese sind voll lizenziert, sind keine betriebssystemeigene Software und werden regelmäßig upgedatet.

---

bca TIPP

Nicht alle Versicherer haben die gleichen Sicherheitsvorschriften. Z.B. besteht die Allianz nicht auf mindestens täglicher Datensicherung. Das könnte für den Kunden entscheidend sein.

A.192.1223

Hotline: Tel.: (0 61 71) 91 50–180, Fax: (0 61 71) 91 50–181, E-Mail: gewerbe@bca.de
BCA AG, Frankfurter Landstraße 62 a, 61440 Oberursel, www.bca.de

Wer wickelt die Schäden ab?

Im Schadenfall ist es wichtig, dass die Versicherer einen guten Krisendienstleister und IT-Sicherheitsexperten zur Verfügung stellen. Es muss schnell gehandelt werden. Sicherheitslücken müssen sofort geschlossen und Daten wiederhergestellt werden. Der Dienstleister muss auch Manpower aufweisen um Kapazitäten frei zu haben. Anbei Informationen von Dienstleistern (ohne Gewähr) die einen guten Eindruck auf uns machen:

metafinanz	(https://metafinanz.de)	Interner Dienstleister der Allianz mit etwa 400 Mitarbeitern
HISOLUTIONS	(https://www.hisolutions.com/)	Dienstleister der HISCOX mit etwa 140 Mitarbeitern in Deutschland und 2.000 weltweit.
msg	(https://www.msg.group/)	Dienstleister von Markel mit etwa 6.000 Mitarbeitern

Datenschutz?

Wir haben die führenden Versicherer Allianz, HISCOX und Markel gefragt, wo die Daten des Versicherers und des Dienstleisters gespeichert werden? Hier die Antworten:

Allianz: Die Daten bei der Allianz werden nur innerhalb Europa gespeichert. Exakt ist es so, dass die Daten der deutschen Allianzgesellschaften in Frankfurt als Master gespeichert werden. Einen Spiegel der Daten als Datensicherung gibt es in Frankreich. Die Rechenzentren und deren Betrieb werden regelmäßig auditiert (Als Audit werden allgemein Untersuchungsverfahren bezeichnet, die dazu dienen, Prozesse hinsichtlich der Erfüllung von Anforderungen und Richtlinien zu bewerten. Dies erfolgt häufig im Rahmen eines Qualitätsmanagements) um eine Einhaltung des Datenschutzgesetzes zu gewährleisten.

HISCOX: Aktuell ist unser Hauptserver in London mit einem Backup in Paris. Auf diese Daten wird über Terminalserver zugegriffen, d.h. darüber hinaus gibt es in den einzelnen Ländern, z.B. in Deutschland, keine lokal gespeicherten Daten.

Markel: Markel Server als auch die Server des Dienstleisters stehen in Deutschland. Weder Markel noch der Dienstleister speichern Kundendaten außerhalb Deutschlands (Hallstadt in Franken).

Gibt es sinnvolle Zusatzabsicherungen?

- **Unternehmens- oder persönliche D&O Versicherung** (ggf. zusätzlich/inklusive einer D&O Selbstbehaltsversicherung für Vorstände einer Aktiengesellschaft)

- **Eigenschadenversicherung:** Erfüllungsgehilfen (Mitarbeiter, Aushilfen, Praktikanten) treffen ebenfalls oft Entscheidungen die zu größeren Schäden führen können. Falsche Bestellungen und vergessene Meldungen können enorme Kosten verursachen.

A.192.1223

Hotline: Tel.: (0 61 71) 91 50–180, Fax: (0 61 71) 91 50–181, E-Mail: gewerbe@bca.de
BCA AG, Frankfurter Landstraße 62 a, 61440 Oberursel, www.bca.de