CyberCrime

Auswirkungen auf das eigene Unternehmen

Je weiter die Digitalisierung fortschreitet, desto größer wird die Angriffsfläche für Gefahren aus dem Netz. Besonders Deutschland mit einem starken, breit aufgestellten und innovativen Mittelstand bietet weltweit eines der attraktivsten Angriffsziele. Digitale Angriffe können den Unternehmen beträchtliche Schäden zufügen. Die Auswirkungen dieser Gefahren sind vielfältig.

Insgesamt beliefen sich die Schäden für deutsche Firmen 2017 auf 110 Mrd. €. Diese Summe beinhaltet z.B. Kosten für Ermittlungen und Ersatzmaßnahmen, Verlust von Wettbewerbsvorteilen, Imageschäden bei Kunden oder Patentrechtsverletzungen. Mittlerweile war bereits jedes zweite deutsche Unternehmen Opfer eines Cyberangriffs. Die Dunkelziffer nicht gemeldeter Angriffe ist hoch. Die Firmen fürchten um ihre Reputation und ihr Image. Laut Risikobarometer 2018 des Allianz Konzerns sind die Cyber-Krisen in der Wahrnehmung der Unternehmensleiter weltweit die Nummer 2 unter den Geschäftsrisiken.

Prävention

Die Implementierung von Maßnahmen für technische, organisatorische und personelle Sicherheit sind ebenso wichtig, wie die Erstellung von Notfall- und Krisenplänen für den Fall der Fälle. Allerdings verfügen ca. 50% aller Unternehmen noch nicht über einen Notfallplan und fast ein Drittel haben keine Sensibilisierungsschulungen in der Belegschaft durchgeführt. Unternehmen benötigen mehr denn je Erkennungs- und vor allem Reaktionsfähigkeiten, um Cyber-Incidents erfolgreich zu bewältigen.

Europäische Datenschutzgrundverordnung

Mit Einführung der EU-DSGVO im Mai 2018 wurde der Schutz personenbezogener Daten neu geregelt. Die Konsequenz daraus ist die Verschärfung und signifikante Erweiterung der Haftung sowie der Kontrollpflichten der Geschäftsleitung. Wegen Nichteinhaltung der neuen Regeln können Geschäftsführer zur Haftung mit Schadenersatz bzw. Geldbußen herangezogen werden (Art. 82 I EU-DSVGO in Verbindung mit § 43 II GmbHG §§ 93 II, 91 II AktG). Schlimmstenfalls drohen strafrechtliche Ermittlungen.

Gemäß Art. 82 I EU-DSGVO hat jede Person, der ein materieller oder immaterieller Schaden entstanden ist, einen Direktanspruch gegenüber dem Verantwortlichen. Erschwerend kommt hinzu, dass bei Ansprüchen Dritter der verantwortliche Geschäftsführer im Rahmen der Umkehr der Beweislast selbst die Beweislast trägt (Art. 82 II EU-DSGVO).

Zur Leistungsaufgabe und Organverantwortung des Vorstandes einer AG (gleiches gilt für GmbH-Geschäftsführer) gehört es, nach besten Kräften dafür zu sorgen, dass das Unternehmen und seine Mitarbeiter „sämtliche Vorschriften einhalten, die das Unternehmen als Rechtssubjekt treffen“:

Die Geschäftsleitung genügt nur dann ihrer Leistungsaufgabe, wenn sie dafür Sorge trägt, „dass das Unternehmen so organisiert und beaufsichtigt wird, dass keine derartigen Gesetzesverletzungen stattfinden“ (vgl. z.B. LG München I, Urteil vom 10.12.2013, Az. 5 HKO 1387/10).

Gesetzliche Struktur

GmbH-Geschäftsführer		Vorstand einer AG	
Innenhaftung	Außenhaftung	Innenhaftung	Außenhaftung
Grundsatz: Geschäftsführer haftet nur ggüb. Gesellschaft § 43 GmbH	Haftung ggüb. einzelnen Gesellschaftern sowie sonstigen Dritten, z. B. § 823 II BGB i.V.m. § 15a I, III InsO	**Grundsatz:** Vorstand haftet nur ggüb. Gesellschaft § 93 II AktG	Haftung ggüb. einzelnen Aktionären (§ 117 I 2 AktG; § 823 II BGB i.V.m.; § 266 StGB bzw. §§ 399, 400 AktG) sowie sonstigen Dritten, z. B. § 93 V AktG

Quelle: RA Dirk Petri, verte | rechtsanwälte

Der Schutz des Unternehmens und seiner Ressourcen gegenüber Cyber-Angriffen gehört eindeutig zur vorgenannten Organverantwortung der Unternehmensleitung.

Umgang mit dem (Rest-)Risiko

Trotz aller professionell durchgeführten Präventiv-Maßnahmen und EDV-Struktur mit entsprechendem Schutz gibt es keine absolute Sicherheit. Die EDV-Struktur sollte zum einen professionell implementiert und zum anderen regelmäßig auf ihren aktuellen Stand überprüft werden.

Aber: die Frage, die sich für den Unternehmensleiter stellt, ist wie er das Restrisiko für sein Unternehmen sichert.

Dabei gilt es zu beachten, dass die Risikofaktoren mehrdimensional sind.

Das Risiko des Eigenschadens, wie bspw. die Wiederherstellung der Systeme oder Betriebsunterbrechung (Umsatzeinbußen) sind ebenso relevant wie Haftpflichtansprüche Dritter z.B. durch Vertraulichkeits-, Datenschutz- und Netzwerkverletzungen. Behördliche Datenschutzverfahren, Support im Krisenfall und Krisenkommunikation sollten im Risk-Management ebenfalls Berücksichtigung finden.

Zusammenfassend lässt sich konstatieren, dass die Unternehmensleiter dieses wichtige Thema in jedem Fall ganzheitlich betrachten sollten. Aktuelle Hard- und Software, juristische Begleitung und für den Notfall ein adäquater EDV-Support, und das alles durch eine abgestimmte Versicherungslösung abgedeckt – bei diesen komplexen Zusammenhängen, die signifikant ineinander greifen, ein absolutes Muss. ■

Dipl.-Volksw. Christos Pechlivanidis (li.)
Dipl.-Kaufm. Michael Jung (r.)
www.cyber-schutz-netzwerk.de