Börsen-Zeitung

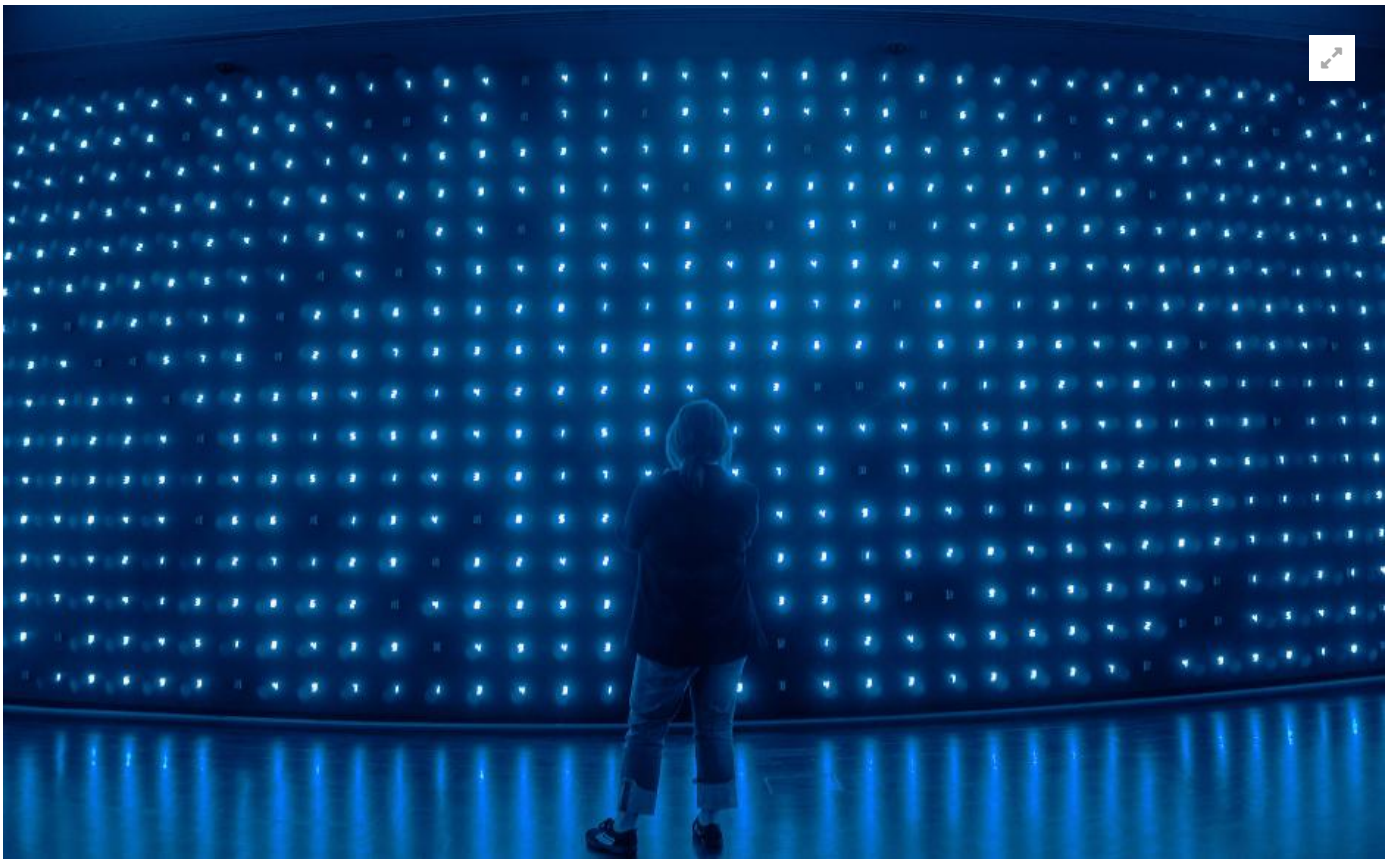
GASTBEITRAG: RANSOMWARE BöZ+

Cyberattacken fordern Manager heraus

Angriffe und Schäden durch Cyberattacken nehmen stark zu. Unternehmen sind zu einem angemessenen Risikomanagement verpflichtet. Wirtschaftliche Folgen können über Cyberversicherungen abgedeckt werden.

München/Düsseldorf, 26.07.2021

Daniel Rücker , Dan Schilbach



© Bildquelle: Yeo Khee/Unsplash

Von Daniel Rücker
und Dan Schilbach *)

In jüngster Zeit häufen sich Medienberichte über Unternehmen und Behörden, die Opfer von Cyberattacken geworden sind. Auch während der pandemiebedingten Verlagerung der Arbeit ins Homeoffice ist die Zahl von Cyberangriffen nochmals massiv gestiegen. Der Angriff auf den IT-Sicherheitsdienstleister Kaseya oder die massenhafte Ausnutzung von Sicherheitslücken in Microsoft-Exchange-Servern demonstrieren anschaulich, dass praktisch jedes Unternehmen zum Opfer von Cyberkriminellen werden kann.

Dabei zählen Ransomware-Angriffe derzeit wohl zu einer der größten Bedrohungen für die IT von Unternehmen und Organisationen. Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern (vor allem durch Verschlüsselung) und mit dem Ziel eingesetzt werden, von den Betroffenen die Zahlung von Lösegeldern zu erpressen. Eine für den Gesamtverband der Deutschen Versicherungswirtschaft erstellte aktuelle Forsa-Umfrage zeigt, dass auch die wirtschaftlichen Schäden durch Cyberattacken exponentiell gestiegen sind. Danach gaben 39 % der betroffenen mittelständischen Unternehmen an,

nach einem Cybervorfall vier oder mehr Tage für die Wiederherstellung ihrer IT-Systeme gebraucht zu haben. In den Vorjahren lag dieser Anteil noch bei 20 %.

Risikomanagement

Aktuelle Studien wie das Allianz Risk Barometer 2021 zeigen, dass Geschäftsführer, Vorstände und Risikomanager von Unternehmen Cyberrisiken mittlerweile zu den größten Geschäftsrisiken zählen – sowohl in Deutschland als auch weltweit. Cyberrisiken gehören deshalb in den Fokus des betrieblichen Risikomanagements. Geschäftsführern und Vorständen von Kapitalgesellschaften kann im Fall einer Cyberattacke unter Umständen sogar eine persönliche Haftung drohen. Werden etwa aufgrund mangelnder Sicherheitsvorkehrungen vertrauliche Kundendaten des Unternehmens durch Hacker entwendet oder fällt eine Produktionsanlage wegen unzureichender Ausstattung und Pflege der IT-Infrastruktur aus und entsteht der Gesellschaft hierdurch ein Schaden, liegt es nahe, insoweit auch eine potenzielle Verantwortlichkeit der Geschäftsleitung in Betracht zu ziehen. Vorstandsmitglieder einer Aktiengesellschaft haben bei ihrer Geschäftsführung gemäß § 93 Abs. 1 AktG die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Ein vergleichbarer Pflichtenmaßstab ergibt sich für GmbH-Geschäftsführer aus § 43 Abs. 1 GmbHG. Teil der allgemeinen Sorgfaltspflichten eines Geschäftsleiters ist es, für ein rechtmäßiges Verhalten des Unternehmens Sorge zu tragen (Legalitätspflicht).

Pflichten zur IT-Sicherheit

Im Bereich der IT-Sicherheit hat der Gesetzgeber in unterschiedlichem Kontext zahlreiche Vorgaben getroffen, die Unternehmen zur Einrichtung eines angemessenen Cyberrisikomanagements verpflichten. Die EU-Datenschutzgrundverordnung (DSGVO) verpflichtet Unternehmen dazu, unter Berücksichtigung u. a. des Stands der Technik geeignete technische und organisatorische Maßnahmen zu treffen, um ein im Einzelfall angemessenes Schutzniveau für die verarbeiteten Daten zu gewährleisten. Daneben bestehen auch spezialgesetzliche Regelungen zur IT-Sicherheit, z. B. für Betreiber kritischer Infrastrukturen oder für andere besonders regulierte Industriezweige wie etwa Banken und Versicherungen.

Vorstand und Aufsichtsrat sind im Rahmen der Legalitätspflicht gehalten, für die Einhaltung dieser gesetzlichen Vorschriften zu sorgen. Darüber hinaus trifft die Geschäftsleitung aber auch eine allgemeine Pflicht, das Thema Cyberrisiken und IT-Sicherheit im Rahmen des Risikomanagements zu validieren und auf dieser Grundlage geeignete Maßnahmen zur Gewährleistung der IT-Sicherheit im Unternehmen zu treffen, um das Risiko von Cyberangriffen und Datenverlusten soweit möglich zu begrenzen.

Die Verpflichtung der Geschäftsleitung, für ein rechtmäßiges Handeln der Gesellschaft Sorge zu tragen, umfasst auch die Einhaltung der DSGVO und die Einrichtung einer unternehmensinternen Datenschutzorganisation. Dabei ist auch sicherzustellen, dass etwaige bei Cyberangriffen erforderliche Melde- und Informationspflichten geprüft und umgesetzt werden. Die DSGVO verpflichtet Unternehmen grundsätzlich, Verletzungen des Schutzes personenbezogener Daten unverzüglich, möglichst binnen 72 Stunden, an die zuständige Datenschutzbehörde zu melden. Das gilt auch dann, wenn die Datenschutzverletzung bei einem Dienstleister auftritt, den das Unternehmen als Auftragsverarbeiter einsetzt.

Solche Auftragsverarbeiter, die für Dritte Daten verarbeiten, müssen etwaige im Rahmen der Auftragsverarbeitung auftretende Datenschutzverletzungen unverzüglich dem jeweiligen Auftraggeber melden. Bei Verstößen gegen diese Pflichten drohen im schlimmsten Fall Bußgelder in Millionenhöhe. Führt die Datenschutzverletzung voraussichtlich zu hohen Risiken für natürliche Personen, deren Daten von einer Cyberattacke betroffen sind, sind diese Personen über den Vorfall unverzüglich zu benachrichtigen. Auch bei Verstößen gegen die Benachrichtigungspflicht drohen hohe Bußgelder.

Für Betreiber kritischer Infrastrukturen bestehen unter bestimmten Voraussetzungen weitergehende Meldepflichten gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Ähnliches gilt für Betreiber bestimmter digitaler Dienste in den Bereichen Cloud Computing, Online-Marktplätze und Online-Suchmaschinen.

Cyberversicherungen

Die Haftungsrisiken, die sich aus der Organtätigkeit als Vorstand oder Geschäftsführer ergeben, lassen sich durch den Abschluss einer D&O-Versicherung zumindest in weiten Teilen absichern. Die D&O-Versicherung erstreckt sich in der Regel auch auf Haftungsrisiken von Geschäftsleitern infolge von Sorgfaltspflichtverletzungen im Umgang mit Cyberrisiken.

Auch die das Unternehmen treffenden wirtschaftlichen Folgen eines Cyberangriffs lassen sich zumindest teilweise über sogenannte Cyberversicherungen absichern. Diese bieten Versicherungsschutz nicht nur für klassische Hackerangriffe, sondern regelmäßig auch für Schäden aus fahrlässigem Umgang der Mitarbeiter mit betrieblich genutzten IT-Systemen. Cyberversicherungen erstrecken sich üblicherweise sowohl auf Eigenschäden des Unternehmens (z.B. durch Betriebsunterbrechung, Aufwendungen zur Wiederherstellung von Daten und IT-Systemen) sowie auf Haftpflichtansprüche, die Dritte im Zusammenhang mit einem Cybervorfall gegen das Unternehmen erheben (z. B. Schadenersatzforderungen wegen Datenschutzverletzungen).

Sorgfältige Analyse sinnvoll

Im Fall von Ransomware-Attacken sind zumeist sogar Zahlungen von Lösegeldern an Cyberkriminelle gedeckt, wobei insoweit stets zu prüfen ist, ob der Zahlung im Einzelfall nationale oder internationale Straf- oder Sanktionsbestimmungen entgegenstehen. Cyberversicherungen decken meist auch Kosten, die bei der Einbindung externer Dienstleister zur Bewältigung einer Cyberattacke entstehen. Dazu zählen z. B. die Kosten für die Tätigkeit von IT-Forensikern zur Aufklärung des Cybervorfalls oder von Rechtsberatern zur Unterstützung bei der Erfüllung gesetzlicher Meldepflichten.

Die Cyberversicherung hat auch im Rahmen des betrieblichen Risikomanagements Bedeutung, weil die Versicherer ihre Versicherungsnehmer im Schadenfall beim Krisenmanagement unterstützen, etwa über eine telefonische Notfall-Hotline und einen direkten Zugang zu einem spezialisierten Krisendienstleister. So helfen sie Unternehmen im Fall einer Cyberattacke auch bei der bestmöglichen Begrenzung von Schäden.

Beim Abschluss einer Cyberversicherung sollten Unternehmen beachten, dass die Vielzahl der am Markt verfügbaren Deckungskonzepte sich bei der Beschreibung des versicherten Risikos, Ausschlüssen und einzelnen Leistungsbausteinen zum Teil erheblich unterscheiden. Vor Abschluss einer Cyberversicherung ist deshalb eine sorgfältige Analyse der Bedingungen zu empfehlen.

**) Dr. Daniel Rücker ist Partner von Noerr in München und Dr. Dan Schilbach Associate im Düsseldorfer Büro der Kanzlei.*

Börsen-Zeitung

© 2021 Börsen-Zeitung – eine Marke der [WM] GRUPPE