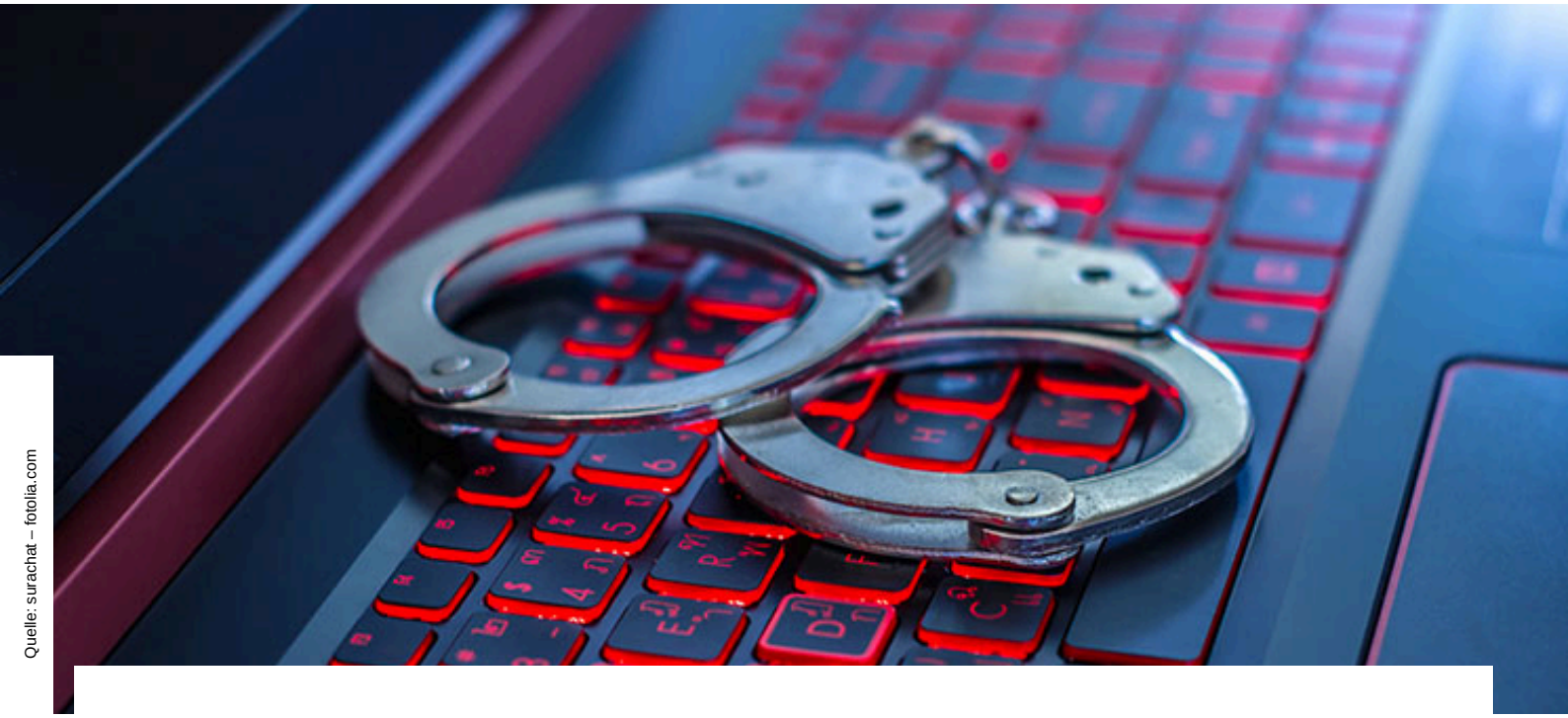

Quelle: surachat – fotolia.com

# Die Rechtsfolgen eines Cyberangriffs

**Im Wesentlichen ist eine Schädigung oder Manipulation der EDV-Systeme zumeist einem verschuldeten Verhalten eines „anderen“ geschuldet. Aufgrund der vertraglichen Konstellationen und der gesetzlichen Rechtslage wird man häufig die Schadenersatzansprüche gegen einen „Schädiger“ geltend machen können. Was ist aber, wenn man diesem Schädiger nicht habhaft werden kann oder wenn dieser einfach kein Vermögen hat?**

## a. Umfang des zu leistenden Schadensersatzes und betroffene Personen

Der durch einen Cyberangriff entstandene Schaden ist nicht begrenzt auf die Kosten, die für das gegebenenfalls notwendige Wiederherstellen von Betriebssystemen anfallen können. Vielmehr erstrecken sich die negativen wirtschaftlichen Folgen auf Umsatzeinbußen, Kosten, welche zur Feststellung der Ursache für den Cyberangriff aufgewendet werden müssen, Ausgaben für technisches Personal und juristische Beratung sowie ein eventuelles Bußgeld (Quelle: Löschhorn/Fuhrmann in NZG 2019, 161, (170), „Neubürger“ und die Datenschutz-Grundverordnung: Welche Organisations- und Handlungspflichten treffen die Geschäftsleitung in Bezug auf Datenschutz und Datensicherheit?).

Nicht zuletzt kann auch der Wert des Unternehmens selbst nachteilig beeinflusst werden (Quelle: Schmidt-Versteyl in NJW 2019, 1637, (1638), Cyber Risks – neuer Brennpunkt Managerhaftung).

Die Gesellschafter eines Unternehmens werden also wenig erfreut sein, wenn derartige außerplanmäßige Kosten entstehen, die durch eine sichere IT hätten vermieden werden können. Daher stellt sich natürlich auch die Frage, ob die Gesellschafter dann Schadensersatzansprüche an die Geschäftsführung haben?

Zu diesen „eigenen“ Kosten des Unternehmens können noch sehr beträchtliche Ausgaben für Schadensersatzzahlungen (also existenzbedrohende!) an Dritte hinzukommen.

Gem. §§ 280 Abs. 1, 2; 286 BGB können Kundinnen und Kunden sowie Lieferantinnen und Lieferanten z.B. bei eintretenden Lieferausfällen, Verzug oder erlittenem Datenverlust das von einem Cyberangriff betroffene Unternehmen in Anspruch nehmen.

Verliert das angegriffene Unternehmen Daten oder werden diese gestohlen, besteht zudem die Möglichkeit der Inanspruchnahme nach § 280 BGB aufgrund der Verletzung von Vertraulichkeitspflichten (Quelle: Schmidt-Versteyl in

NJW 2019, 1637, (1638), Cyber Risks – neuer Brennpunkt Managerhaftung).

Aufgrund der Verschuldensvermutung aus § 280 Abs. 1 S. 2 BGB ist es Aufgabe des Unternehmens, nachzuweisen, dass den IT-bezogenen Sicherheitspflichten in einem hinreichenden Maße zuvor nachgekommen wurde. Es ist also eine wichtige Aufgabe der Geschäftsführung, eine ordnungsgemäße Dokumentation der IT nachzuweisen, als dass diese dem Stand der Technik entspricht.

Daneben tritt Art. 82 DSGVO. Hieraus resultiert für das personenbezogene Daten verarbeitende Unternehmen die Haftung hinsichtlich materieller und immaterieller Schäden, die auf eine nicht DSGVO-konforme Verarbeitung personenbezogener Daten zurückgehen (Quelle: Löschhorn/ Fuhrmann in NZG 2019, 161, (169), „Neubürger“ und die Datenschutz-Grundverordnung: Welche Organisations- und Handlungspflichten treffen die Geschäftsleitung in Bezug auf Datenschutz und Datensicherheit?).

Insbesondere bei der Entwendung personenbezogener Daten kann der zu ersetzende immaterielle Schaden den materiellen Schaden durchaus übersteigen (Quelle: Schmidt-Versteyl in NJW 2019, 1637, (1638), Cyber Risks – neuer Brennpunkt Managerhaftung). Eine Exkulpationsmöglichkeit besteht nur, wenn den Verantwortlichen der Nachweis gelingt, dass sie „in keinerlei Hinsicht“ für den Schaden auslösenden Faktor Verantwortung tragen.

Zu der Haftung aus Art.82 DSGVO tritt die Möglichkeit, dass eine Geldbuße nach Art. 83 DSGVO verhängt wird. Die Geldbußen sollen „im Einzelfall wirksam, verhältnismäßig und abschreckend “ sein. Eine Geldbuße kann daher bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes im vergangenen Geschäftsjahr betragen (Rubin in r+s 2018, 337, (341), Inhalt und versicherungsrechtliche Auswirkungen der Datenschutz-Grundverordnung), im Falle von Google zum Beispiel über 50 Millionen Euro (Schmidt-Versteyl in NJW 2019, 1637, (1638), Cyber Risks – neuer Brennpunkt Managerhaftung).

In Deutschland wurde wohl im Jahre 2019 das höchste Bußgeld gegenüber dem Unternehmen Deutsche Wohnen verhängt. Das Bußgeld betrug 14,5 Milliarden Euro, weil eine ordnungsgemäße Datenlöschung nicht gewährleistet wurde.

Sie können aber auch das Bußgeld für Ihr Unternehmen schnell ermitteln, indem Sie ihren Jahresumsatz nehmen und diesen durch 360 Tage teilen. Etwa das Zehnfache des daraus resultierenden Tagessatzes wird als angemessen angesehen. Dieses ist die voraussichtlich künftige Handhabung, wie die individuelle Höhe eines Bußgeldes als „Ausgangswert“ bestimmt wird. Natürlich gibt es auch noch verschärfende oder mildernde zu berücksichtigende Faktoren. Es ist aber eine gute „Daumenregel“ um die voraussichtliche Höhe des Bußgeldes für einen Datenschutzverstoß zu ermitteln. Leider ist es nur so, dass „Schadenzahlungen“ für Bußgelder nicht versicherbar sind. Daher muss die Geschäftsführung insbesondere die Einhaltung dieser gesetzlichen Vorschriften sicherstellen.

## b. Kein Ausschluss durch AGB

Die Verantwortlichkeit von Geschäftsführerinnen und Geschäftsführern kann auch nicht durch Verwendungen von AGB begegnet werden, welche Haftungsbeschränkungen zum Inhalt haben. Werden AGB verwendet, so haben die Verwendenden dennoch für vorhersehbare Schadensfolgen im Bereich der wesentlichen Vertragspflichten einzustehen. Lieferpflichten nachzukommen und Kundendaten vertraulich zu behandeln, stellen wesentliche Vertragspflichten dar, sodass ein Haftungsausschluss für den Fall fahrlässiger Verstöße höchstens durch individualvertragliche Vereinbarung in Betracht kommt (Quelle: Schmidt-Versteyl in NJW 2019, 1637, (1638), Cyber Risks – neuer Brennpunkt Managerhaftung).

## c. Rückgriff auf Mitarbeiterinnen und Mitarbeiter kaum realisierbar

Obwohl eine Vielzahl von Cyberangriffen erst durch Anwenderfehler möglich wird, ist die Inanspruchnahme von Mitarbeiterinnen und Mitarbeitern des eigenen Unternehmens bei betrieblich veranlasster Tätigkeit oft nicht erfolgsversprechend, da eine Haftung dieser bei fahrlässigem Handeln beschränkt ist (Quelle: Vgl. Fortmann in r+s, 2019, 688, (693), Cyber-Datenrisiken: Erhebliche Gefahr für Geschäftsleiter und D&O-Versicherer?).

Auch bei grob fahrlässigen Pflichtverletzungen hat das BAG Arbeitnehmerinnen und Arbeitnehmern bisher keine Haftungsquote auferlegt, die deren Jahresgehalt übersteigt (Quelle: Schmidt-Versteyl in NJW 2019, 1637, (1639), Cyber Risks – neuer Brennpunkt Managerhaftung). Durch Cyberangriffe eintretende Schäden können diese Summen jedoch leicht um ein Vielfaches überschreiten. Zu bedenken ist auch, dass nach den im Arbeitsrecht geltenden Grundsätzen der Mitarbeiterin oder dem Mitarbeiter Verschulden nachgewiesen werden muss und nicht umgekehrt.

Mit anderen Worten die Geschäftsführung und die Unternehmung hat für etwaiges Fehlverhalten ihrer Mitarbeiter einzustehen. Selbst wenn ein Rückgriff gegenüber einem Mitarbeiter theoretisch möglich wäre, so greift eine strikte Haftungsbegrenzung, als dass in der Regel kaum mehr als drei Monatsgehälter geltend gemacht werden können. Ein wirtschaftlich nachhaltiger Rückgriff auf den Verursacher, der als Mitarbeiter grob fahrlässig gehandelt hatte, ist also unter wirtschaftlichen Gesichtspunkten nicht gegeben.

## d. Kein Rückgriff auf IT-Dienstleisterinnen und -Dienstleister

Auch die Inanspruchnahme der das Unternehmen unterstützenden IT-Dienstleisterinnen und -Dienstleister wird häufig erfolglos verlaufen, da diese in der Regel „nur“ die vertraglich vereinbarten Aufgaben als Hauptleistungen zu erbringen haben. Die vertraglich vereinbarten Aufgaben können auch häufig deutlich unter dem „Stand der Technik“ liegen. Daher kommt es vermutlich häufig vor, dass aus Unkenntnis der Geschäftsführung oder mangelnden finanziellen Rahmen der Firma nur technisch notwendige Dienstleistungen vorgenommen werden, die nicht dem sich wandelnden „Stand der Technik“ entsprechen.

Das Erfordernis aber zum Betrieb einer IT nach „Stand der Technik“ ergibt sich aus Art. 24 Abs. 1 u. 2 DSGVO und der daraus resultierenden Verpflichtung, auch den Nachweis hierfür erbringen zu können (s. auch ErwGrd 74). Daher bedarf es auch einer nachvollziehbaren Dokumentation.

Sofern es an einer solchen vertraglichen Verpflichtung des IT-Dienstleisters fehlt, hat er also allenfalls die Nebenpflicht zu erfüllen, die Geschäftsführung auf die nach Art. 24 DSGVO erforderlichen technischen Maßnahmen (TOM’s) hinzuweisen, die dem jeweiligen „Stand der Technik“ entsprechen. Wird diese Beratungsverpflichtung nicht erfüllt, so ist es natürlich vorstellbar, dass der IT-Dienstleister wegen der Verletzung von Beratung und Aufklärungspflichten schadenersatzpflichtig gemacht werden könnte (§ 280 BGB). Dennoch besteht natürlich das Problem, einen möglicherweise sehr hohen Forderungsanspruch auch tatsächlich erfolgreich gegenüber dem IT-Dienstleister durchzusetzen und zu vollstrecken.

Des Weiteren werden im Rahmen größerer Verträge regelmäßig prozentuale oder betragsmäßige Haftungsgrenzen vereinbart.

Auch die Inanspruchnahme von Softwareherstellern oder deren Vertrieb für die dem Grunde nach virusanfällige Software ist nur schwierig realisierbar, da Sicherheitslücken in vielen Fällen erst nach Kauf erkennbar werden und die Verkäuferinnen und Verkäufer sich entlasten können, wenn das Produkt zum Herstellungszeitpunkt dem „Stand der Technik“ entsprach. Oder diese, wie beispielsweise Microsoft oder Google gar nicht so einfach juristisch greifbar sind.

Handelt es sich bei der Verkäuferin oder dem Verkäufer um eine Zwischenhändlerin oder einen Zwischenhändler, was regelmäßig der Fall sein wird, so sind diese hinsichtlich des Bestehens von Sicherheitslücken im Grundsatz auch nicht zur Produktbeobachtung verpflichtet (Quelle: Schmidt-Versteyl in NJW 2019, 1637, (1639), Cyber Risks – neuer Brennpunkt Managerhaftung).

https://www.experten.de/2020/03/02/haftung-der-geschaeftsfuehrer-bei-einem-cyberangriff/

Versicherungs- und Finanznachrichten

# expertenReport

https://www.experten.de/id/4918729/die-rechtsfolgen-eines-cyberangriffs/