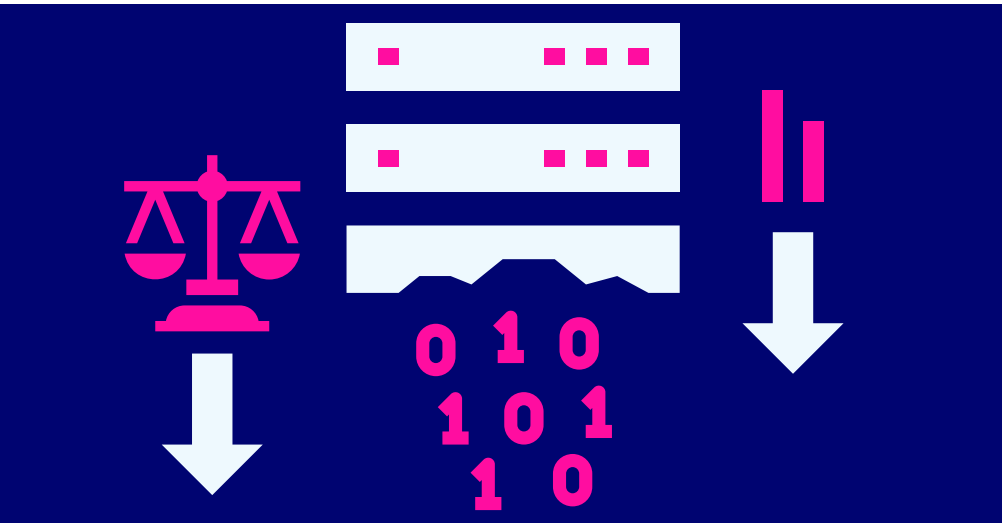

Das lukrative Geschäft mit Schadensersatzklagen

Neben Datenklau und Erpressung entwickeln sich auch konzertierte Schadensersatzforderungen Betroffener zu einer Bedrohung für Unternehmen. Ein Argument mehr, den Datenschutz ernst zu nehmen.

Von Dr. Hauke Hansen und Carsten Wiesenthal

Cyberattacken stellen für Unternehmen eine immer größere Gefahr dar. Sind die Angreifer erfolgreich in die IT-Systeme eingedrungen, werden die Daten verschlüsselt und der Geschäftsbetrieb und die Produktion lahmgelegt. Außerdem ziehen die Täter Daten ab und erpressen das Unternehmen. Lehnt es eine Lösegeldzahlung ab, werden die Unternehmensdaten im Darknet veröffentlicht oder dort zum Kauf angeboten. Die Folgen eines solchen Datenlecks können enorm sein und nicht selten das Bestehen des Unternehmens gefährden. Neben möglichen Bußgeldern von Datenschutzbehörden entwickeln sich auch orchestrierte Schadensersatzansprüche von betroffenen Kunden zu einer ernst zu nehmenden Bedrohung.

Die Datenschutz-Grundverordnung der EU verpflichtet Unternehmen durch ihren Artikel 32 dazu, angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu ergreifen. Seitdem haben Datenschutzbehörden in Deutschland und zahlreichen anderen EU-Ländern Geldbußen in Millionenhöhe verhängt. Die genaue Höhe der Strafen hängt von verschiedenen Faktoren ab, einschließlich der Fähigkeiten der Angreifer, der Qualität der bestehenden IT-Sicherheitsinfrastruktur, der Größe des Unternehmens und der Art der personenbezogenen Daten, die betroffen sind. In allen EU-Ländern können die Datenschutzbehörden Geldbußen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes des betroffenen Unternehmens verhängen, je nachdem, welcher Betrag höher ist.

Unternehmen haften auch zivilrechtlich

Neben der Verfolgung durch eine Behörde können Unternehmen allerdings auch zivilrechtlich haftbar gemacht werden, beispielsweise in Form von Klagen auf Schadensersatz. Wenn die Hacker Kundendaten oder Daten von Mitarbeitern im Darknet veröffentlichen, dient den Betroffenen Artikel 82 der DSGVO als Grundlage einer Klage. Einen solchen Schadensersatzanspruch haben die Kunden theoretisch auch gegen die Kriminellen. Aber die sind in aller Regel nicht bekannt und nicht greifbar. Also stellt sich für die betroffenen Kunden die Frage, ob nicht auch die angegriffenen Unternehmen für einen eingetretenen Schaden einstehen müssen. Dass die Unternehmen als Opfer einer Cyberattacke auch auf diesem Wege zur Kasse gebeten werden sollen, mutet überraschend an – die DSGVO sieht solche Ansprüche jedoch vor.

Um Anspruch auf Schadensersatz zu haben, müssen betroffene Personen nachweisen können, dass sie einen materiellen oder neuerdings auch immateriellen Schaden durch einen Datenschutzverstoß erlitten haben. Ein solcher Verstoß kann schon in unzureichenden IT-Sicherheitsmaßnahmen der angegriffenen Unternehmen gesehen werden, die nicht dem Stand der Technik entsprechen, wie er beispielsweise durch den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) definiert wird.

Ersatz für immaterielle Schäden – vergleichbar mit einem Schmerzensgeld bei Körperverletzungen oder Beleidigungen – bezieht sich auf Schäden, die keine unmittelbaren finanziellen Folgen haben, etwa das verloren gegangene Vertrauen in ein Unternehmen oder der Verlust der Kontrolle über sehr persönliche Informationen wie Bank- oder Gesundheitsdaten. Trotzdem gibt es noch keine

iX-TRACT

- Cyberangriffe werden für Unternehmen schnell zur existenziellen Bedrohung: Neben Datendiebstahl und Erpressung durch Kriminelle hat die Klageindustrie Schadensersatzklagen von Betroffenen als neues Geschäftsmodell für sich entdeckt.
- Noch sind die Gerichte in der Handhabung uneins, ob ein konkreter Schaden erst bewiesen werden muss oder den vom Datendiebstahl Betroffenen grundsätzlich Schadensersatz zusteht. Das Geschäftsmodell Datenschutzschadensersatzklage hängt von der Entscheidung des EuGH ab, dem Fragen zur Auslegung des einschlägigen Paragrafen der DSGVO vorliegen.
- Gerade kleine und mittlere Unternehmen sind gut beraten, sich externe Sicherheits- und Datenschutzkompetenz ins Haus zu holen und sich rechtzeitig für den Ernstfall finanziell abzusichern.

einheitliche Meinung dazu, ob und in welchem Umfang betroffene Personen Schadensersatzansprüche geltend machen können. Insbesondere ist unter den Gerichten umstritten, ob ein immaterieller Schaden bereits dann vorliegt, wenn Datenschutzvorschriften verletzt wurden, oder ob zusätzlich ein tatsächlich nachweisbarer materieller Schaden wie ein finanzieller Verlust oder ein immaterieller Schaden wie Ärger und Ängste entstanden sein muss.

Schwierige Schadensbemessung

Welche Entschädigung ist angemessen, wenn eine E-Mail-Adresse in den Händen von Spammern und Internetbetrügern landet? Wenn persönliche Details wie Adresse, Geburts- oder Kontodaten im Darknet kursieren? Wenn die Betroffenen mit dem Risiko leben müssen, dass in ihrem Namen nicht existierende Produkte verkauft oder Konten eröffnet werden?

In Deutschland wurden bisher über 130 Urteile zu Artikel 82 DSGVO veröffentlicht. In etwa 30 Prozent dieser Fälle wurde den Klägern Schadensersatz zugesprochen, während die restlichen Klagen abgewiesen wurden. Der Grund: Viele Gerichte sehen den Anspruch aus Artikel 82 DSGVO als klassische Kompensationsfunktion an; sie weisen die Klage ab, wenn lediglich ein individuell empfundenes Unbehagen ohne objektiv nachvollziehbare Beeinträchtigung vorliegt. Andere Gerichte sind hingegen der Ansicht, die rechtlichen Hürden für einen Zahlungsanspruch seien gering, weil von der DSGVO eine abschreckende Wirkung ausgehen müsse, die die Unternehmen diszipliniere.

Im Falle des erfolgreichen Hackerangriffs auf einen Dienstleister des Vermögensverwalters Scalable Capital hat das Landgericht München einem Kunden, dessen Daten von den Hackern veröffentlicht wurden, einen Schadensersatzanspruch in Höhe von 2500 Euro zugesprochen – und das trotz TÜV-zertifizierter IT-Sicherheit beim Dienstleister. Der Kläger wurde von dem Prozessfinanzierer EuGD (Europäische Gesellschaft für Datenschutz mbH) unterstützt, weitere Klagen wurden an mehreren deutschen Gerichten eingereicht. Berücksichtigt man, dass von der Datenpanne insgesamt rund 33 200 Personen betroffen waren, entsteht ein Risiko in Millionenhöhe.

Massenklagen als Geschäftsmodell

Da die einzelnen Ansprüche in diesen Fällen eher von geringer Höhe sind, lohnt sich das Tätigwerden für die kommerziellen Kläger erst in der Masse – ähnlich wie im Falle von Fluggast- oder Mieterrechten. Diese Entwicklungen haben das Interesse der Klageindustrie geweckt. Es gibt mittlerweile eine Vielzahl von Anwaltskanzleien, die sich auf die Durchsetzung von Schadensersatzansprüchen im Zusammenhang mit Datenschutzverletzungen spezialisiert haben.

Hierbei handelt es sich oft um gut organisierte Verbraucherkanzleien, die von ihren Erfahrungen mit Massenverfahren in Zusammenhang mit dem Diesel-Skandal oder der Insolvenz der US-amerikanischen Bank Lehman Brothers profitieren wollen, aber auch Prozessfinanzierer und Legal-Tech-Unternehmen mischen auf dem Markt mit. Dienstleister wie RightNow („Verkaufe dein Problem“) werben gezielt um betroffene Kunden oder Mitarbeiter der gehackten Unternehmen und nutzen die Möglichkeit, aus Datenlecks und ähnlichen Vorfällen Profit zu machen. Prozessfinanzierer übernehmen dabei die Kosten für den Kläger und erhalten im Erfolgsfall eine Provision.

Die Strategie sieht dabei nicht vor, jeden Fall vor Gericht zu bringen, sondern das betroffene Unternehmen zu einem außergerichtlichen Vergleich zu bewegen. Ein Beispiel für den Erfolg dieser Methode ist die Vereinbarung mit Mastercard im Januar 2023, bei der Kunden aufgrund einer illegalen Veröffentlichung von Kundendaten im Zusammenhang mit dem „Mastercard Priceless Specials“-Datenleck jeweils 300 Euro erhielten. Ein Prozessfinanzierer vertrat 2000 von insgesamt 90 000 betroffenen Kunden und erhielt eine Provision von 25 Prozent.

Die Kommerzialisierung der datenschutzrechtlichen Schadensersatzansprüche hat begonnen. Gerade nach Cyberattacken stellen Schadensersatzforderungen ein Risiko für die betroffenen Unternehmen dar. Der zukünftige Erfolg des Geschäftsmodells Datenschutzschadensersatzklage hängt aber von der Auslegung des Artikels 82 DSGVO durch den Europäischen Gerichtshof (EuGH) ab, bei dem derzeit zahlreiche Fragen zur Auslegung des Artikels 82 DSGVO anhängig sind.

Anfang Mai wird er in einem ersten Verfahren entscheiden, ob Bürger nur dann eine Entschädigung erhalten sollen, wenn ihnen konkret messbare Schäden entstanden sind, oder ob bereits das Unwohlsein über eine Datenschutzverletzung ausreicht (Az. C-300/21). Der Generalanwalt beim EuGH – hierbei handelt es sich um eine Art Gutachter, der das Gericht unterstützt – hat in seinen Schlussanträgen im Oktober letzten Jahres zu diesem Fall die Ansicht vertreten, ein bloßer Ärger über eine rechtswidrige Datenverarbeitung führe nicht zu einem Schadensersatzanspruch. Die Richter sind nicht an die Empfehlungen des Generalanwalts gebunden, folgen ihnen aber oftmals.

Rechtzeitig absichern

Für Unternehmen lassen sich diese möglicherweise existenzbedrohenden finanziellen Risiken durch entsprechende Versicherungen absichern. Zum einen durch spezielle Cyberversicherungen, die unter anderem im Hinblick auf die beschriebenen Schadensersatzforderungen und die möglichen behördlichen Bußgelder einspringen. Aber auch ohne Cyberversicherung können die Schäden durch eine bestehende (IT-)Haftpflichtversicherung abgedeckt sein. Selbst Versicherungen fehlen aufgrund des relativ neuen Phänomens der Cyberangriffe oftmals noch einschlägige Erfahrungswerte bei der Risikoermittlung und des konkreten Kundenbedarfs.

Klar ist, dass gerade im Mittelstand insbesondere Servicekomponenten, etwa IT-Sicherheitstrainings für Mitarbeiter, toolbasierte Risikobewertung und vor allem Unterstützung in der Krise durch Vermittlung von Sicherheitsexperten extrem wichtig sind. Dies schon deshalb, weil die Kernkompetenz vieler gerade mittelständischer Unternehmen häufig nicht die IT-Sicherheit des eigenen Betriebes ist. (ur@ix.de)

DR. HAUKE HANSEN

ist Partner der Wirtschaftskanzlei FPS in Frankfurt a. M., Experte für Cybersicherheit, IT-Recht und Datenschutz und entwirft Strategien, um Unternehmen vor Cyberattacken und ihren Folgen zu schützen.

CARSTEN WIESENTHAL

arbeitet bei der ALLCURA Versicherungs-Aktiengesellschaft, ist Rechtsanwalt und seit 2001 in führenden Positionen der Versicherungsindustrie unter anderem für die Bereiche Cyber und IT-Haftpflicht tätig.