| RECHT UND STEUERN |

Weckruf des BGH zur IT-Sicherheit

Das Urteil wegen des Datenlecks bei Facebook hat weitreichende Folgen. Cybersecurity muss in Unternehmen zur Chefsache werden.

Von Hauke Hansen und Lars Kroll

In einer viel beachteten Grundsatzentscheidung hat der Bundesgerichtshof (BGH) jüngst die Schadenersatzhürden für Kunden von Facebook & Co. gesenkt, die ihre vertraulichen Accountdaten wie Telefonnummern frei im Internet wiederfanden. Unabhängig davon, ob dadurch ein konkreter Schaden eingetreten sei, löse allein der zeitweilige Kontrollverlust über die Daten eine Art Schmerzensgeldanspruch aus, befanden die BGH-Richter (Az: VI ZR 10/24).

Neben diesem Schmerzensgeldanspruch nach dem Gießkannenprinzip können betroffene Kunden auch höhere Schadenersatzforderungen stellen – allerdings nur gegen Nachweis des konkreten Schadens. Die Schlüsselfrage lautet dann: Hat das jeweilige Unternehmen ausreichende technische und organisatorische Maßnahmen (TOMs) ergriffen, um Datenlecks zu verhindern.

Cyberattacken stellen für Unternehmen eine große 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, wie das Beispiel Varta zeigt. Der Batterienhersteller durchläuft nach einem Cyberangriff und einem wochenlangen Stillstand der Produktion derzeit ein Restrukturierungsprogramm, an dem auch Porsche beteiligt ist.

Veröffentlichen Hacker Kundendaten oder Daten von Mitarbeitern im Darknet, dient den Betroffenen Artikel 82 der europäischen Datenschutz-Grundverordnung (DSGVO) als Grundlage einer Klage. Theoretisch besteht ein solcher Schadenersatzanspruch auch gegen die Kriminellen. Aber die sind in aller Regel nicht greifbar. Also wenden die Kunden sich an die gehackten Unternehmen. Dass Betriebe als Opfer einer Cyberattacke auch auf diesem Wege zur Kasse gebeten werden sollen, mutet überraschend an, aber die DSGVO sieht solche Ansprüche vor. Grundlage ist der Vorwurf, das Unternehmen hätte sich nicht ausreichend um die IT-Sicherheit gekümmert. Erstattet werden können nicht nur finanzielle Schäden durch den konkreten Missbrauch der erbeuteten Daten, sondern auch immaterielle Schäden. Einen solchen Anspruch kennt man im deutschen Recht vom Schmerzensgeld.

Die Möglichkeit, mithilfe der DSGVO selbst für geringe Datenschutzverstöße Geld einzuklagen, hat das Interesse der Klageindustrie geweckt. Es gibt mittlerweile zahlreiche Anwaltskanzleien, die sich auf die Durchsetzung von Schadenersatzansprüchen im Zusammenhang mit Datenschutzverletzungen spezialisiert haben. Oft handelt es sich um gut organisierte Verbraucherkanzleien, die von ihren Erfahrungen mit Massenverfahren im Zusammenhang mit dem Dieselskandal oder der Insolvenz der US-amerikanischen Bank Lehman Brothers profitieren wollen und nun ein neues Betätigungsfeld suchen. In dieser Branche wurde das Facebook-Urteil des BGH daher auch euphorisch begrüßt. Unternehmen müssten sich gar auf Hunderttausende Datenschutzklagen einstellen, so die Werbebotschaft.

Das Urteil enthält für betroffene Unternehmen auch etwas Positives: Der BGH hat solchen Massenverfahren, unter denen auch die Gerichte ächzen, etwas den Wind aus den Segeln genommen. Für den Kontrollverlust der bei Facebook gespeicherten Daten halten die BGH-Richter einen Ausgleich von 100 Euro für ausreichend. Für höhere Beträge müssen die Kläger konkrete Beeinträchtigungen nachweisen. In den meisten Fällen dürfte die zu erwartende Summe so niedrig sein, dass die betroffenen Unternehmen darauf hoffen können, dass sich nur wenige potentielle Kläger die Mühe machen werden, einen Anwalt einzuschalten.

Gleichwohl kann die neue Rechtsprechung für Unternehmen zu einer Belastung werden. Auf massenhafte Klagen muss reagiert werden, dies bindet Res-

[illegible] ist dabei, das Unternehmen gut gegen Cyberangriffe abzusichern. Zwar verlangen die Gesetze keine einhundertprozentige Sicherheit. Aber europäische Vorschriften wie die Richtlinie NIS-2 zur Netzwerk- und Informationssicherheit erhöhen die Anforderungen an Zehntausende deutsche Unternehmen und führen sogar eine persönliche Haftung der gesamten Geschäftsleitung bei unzureichenden IT-Sicherheitsmaßnahmen ein. Dazu gehören auch eine fehlende Sensibilisierung und Schulung der Mitarbeiter.

Unternehmen sollten außerdem bedenken, dass Datenlecks in Windeseile über Jahre aufgebaute Reputation zerstören können. Unternehmen sollten also zwingend in die IT-Sicherheit investieren; Cybersecurity muss zur Chefsache gemacht und vorgelebt werden. Wenn die Gerichte die umgesetzten Sicherheitsmaßnahmen nach dem Stand der Technik für ausreichend halten, haben Schadenersatzklagen selbst bei erfolgreichen Hackerangriffen keinen Erfolg.

Das letzte Wort im Fall Facebook ist im Übrigen noch nicht gesprochen. Der BGH hat das Verfahren an das Oberlandesgericht Köln zurückverwiesen. Das OLG soll feststellen, ob die technischen Schutzmaßnahmen auf Facebook unzureichend waren. Womöglich nimmt das Verfahren auch noch eine ganz neue Wendung: wenn nach Ansicht des OLG Köln die neue Rechtsprechung des Bundesgerichtshofs nicht mit der Sichtweise des Europäischen Gerichtshofs (EuGH) übereinstimmt. In diesem Fall könnte das Verfahren auch vom OLG Köln an den EuGH verwiesen werden. Mit einer rechtskräftigen Entscheidung wäre dann erst in etwa zwei Jahren zu rechnen.

Hauke Hansen ist Partner der Kanzlei FPS und Lars Kroll Geschäftsführer der Kroll Strategieberatung.