BGH-Urteil: So schützen Unternehmen ihre Daten

In einer Entscheidung zum Datendiebstahl bei Facebook machte der Bundesgerichtshof deutlich, dass schon der Verlust der Kontrolle über die eigenen Daten Schadensersatzansprüche für die Betroffenen begründen kann. Unternehmen müssen umfassende Schutzmaßnahmen für ihre IT treffen und dies auch nachweisen können.

Von Dr. Hauke Hansen und Marek Stiefenhofer

Die Entscheidung des Bundesgerichtshofs (BGH) vom 18. November 2024 zu einer schweren Datenschutzlücke bei Facebook sollte Unternehmen landauf landab zu signifikanten Nachbesserungen an ihrer Datensicherheitsarchitektur veranlassen. Vor einem Laissez-faire-Führungsstil sei gewarnt, denn genau darauf hat es die Klageindustrie abgesehen. Worauf es jetzt beim Datenschutzmanagement und der IT-Compliance ankommt.

Im Mittelpunkt der Grundsatzentscheidung aus Karlsruhe (Az. VI ZR 10/24) steht ein Vorfall, bei dem personenbezogene Daten von Facebook-Nutzern durch eine Sicherheitslücke offengelegt wurden. Bereits der bloße Kontrollverlust über personenbezogene Daten rechtfertigt einen Schadensersatzanspruch gegen das Unternehmen – und zwar unabhängig vom Nachweis einer darüber hinausgehenden konkreten Beeinträchtigung, so der BGH. Unternehmen haften in Zukunft nur dann nicht, wenn sie angemessene Maßnahmen zur Gewährleistung der IT-Sicherheit getroffen haben. Hinzu kommt: Durch neue Gesetze wird die Messlatte nochmals höher gelegt.

iX-TRACT

- Für Unternehmen bedeutet das wegweisende Urteil des BGH gegen Facebook, dass Datenleaks künftig sehr teuer werden können. Schon der bloße Verlust der Kontrolle über die eigenen Daten kann für Nutzer einen Schadensersatzanspruch gegenüber dem Unternehmen auslösen.
- Von Kanzleien, die sich auf die Durchsetzung von Schadensersatzansprüchen spezialisiert haben, sind bei Datenschutzverletzungen Massenverfahren zu erwarten.
- Unternehmen können sich dadurch absichern, dass sie die Daten ihrer Kunden und Nutzer bestmöglich schützen, ihre Mitarbeiter sensibilisieren und alle ergriffenen Maßnahmen sorgfältig dokumentieren.

Risiken für Unternehmen steigen

Bei Cyberangriffen ziehen Täter häufig Daten ab, um sie im Darknet zu veröffentlichen oder zu verkaufen. Neben möglichen Bußgeldern von Datenschutzbehörden entwickeln sich auch orchestrierte Schadensersatzansprüche von betroffenen Kunden zu einer ernst zu nehmenden Bedrohung. Veröffentlichen Hacker Kundendaten oder Daten von Mitarbeitern, dient den Betroffenen Artikel 82 der EU-Datenschutz-Grundverordnung (DSGVO) als Grundlage einer Klage (siehe dazu ein Urteil des EuGH; ix.de/zvh3). Hauptvorwurf ist dann regelmäßig, das Unternehmen habe 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, vergleichbar dem Schmerzensgeld.

Geschäftsmodell massenhafte Datenschutzklagen

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 Schadensersatzansprüchen im Zusammenhang mit Datenschutzverletzungen spezialisiert haben. Oft handelt es sich um gut organisierte Verbraucherkanzleien, die von ihren Erfahrungen mit Massenverfahren beim 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.

Dazu kommt: Der Verbraucherzentrale Bundesverband (vzbv) hat gerade eine Sammelklage gegen die Facebook-Mutter Meta eingereicht. Von der Datenschutzlücke betroffen sind Schätzungen zufolge rund sechs Millionen Menschen in Deutschland. Mit der Sammelklage will der vzbv verhindern, dass mögliche Ansprüche von Verbraucherinnen und Verbrauchern zum Jahreswechsel ver-

jähren. Das Verfahren wird sich über Jahre hinziehen, am Image des betroffenen Unternehmens nagen und viele Ressourcen binden. Auch die neue Rechtsprechung des BGH, der im konkreten Fall einen geringen Schadensersatz von lediglich 100 Euro pro Fall für angemessen hielt, kann für Unternehmen zu einer Belastung werden. Auf massenhafte Klagen muss reagiert werden, dies kostet Arbeitszeit und Geld.

Prävention ist die beste Verteidigung

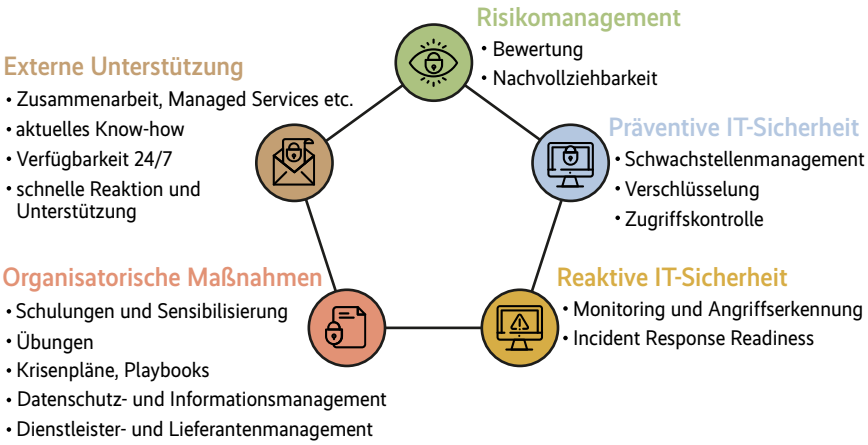
Die beste Verteidigungsstrategie ist daher, das Unternehmen gut gegen Cyberangriffe abzusichern. Zwar verlangen die Gesetze keine einhundertprozentige Sicherheit. Aber europäische Vorschriften wie die DSGVO und darüber hinaus künftig die NIS2-Richtlinie zur Netzwerk- und Informationssicherheit erhöhen die Anforderungen an Zehntausende deutsche Unternehmen. NIS2 führt sogar eine persönliche Haftung der gesamten Geschäftsleitung bei unzureichenden IT-Sicherheitsmaßnahmen ein, wozu auch eine fehlende Sensibilisierung und Schulung der Mitarbeiter gehört.

Wenn die Gerichte die umgesetzten Sicherheitsmaßnahmen nach dem Stand der Technik für ausreichend halten, haben Schadensersatzklagen selbst bei erfolgreichen Hackerangriffen keinen Erfolg. Die beste Verteidigung gegen massenhafte Klagen liegt also in der Prävention. Artikel 32 DSGVO fordert Unternehmen auf, angemessene technische und organisatorische Maßnahmen zu implementieren. Doch was bedeutet das konkret? Die in der Abbildung zusammengefassten wichtigsten Maßnahmen werden im Folgenden beschrieben.

Kernpunkt vieler Regulierungen ist das **Risikomanagement,** das zunächst eine Bewertung der Risiken erfordert. Dazu müssen auch kleinere Organisationen Prozesse und Methoden etablieren, um die Auswirkungen von Sicherheitsvorfällen auf die Geschäftstätigkeit verstehen und bewerten zu können. Manche Risiken können grundsätzlich nicht beseitigt werden, andere nicht zeitnah. Umso wichtiger ist es, die Entscheidungen dazu nachvollziehbar zu begründen, zu dokumentieren und formal durch die Geschäftsleitung freigeben zu lassen.

Schwachstellen managen, Datenzugriffe beschränken

Ein weiterer wichtiger Baustein des Datenschutzes ist die **präventive Sicherheit.** Dazu gehört zwingend ein Schwachstellenmanagement: IT-Systeme müssen regelmäßig geprüft und kritische Sicherheitslücken umgehend geschlossen werden. Nicht geschlossene Sicherheitslücken als Ursache eines Datenschutzvorfalls stellen künftig ein noch höheres Haftungsrisiko dar, insbesondere dann, wenn nachweislich ein Patch oder Workaround zur Verfügung stand. Eine Kombination aus automatisierten Schwachstellenscans und manuellen Penetrationstests mit verschiedenen Blickwinkeln, bis hin zum Red Teaming, ist hier das Mittel der Wahl.



Überblick über die wichtigsten technischen und organisatorischen Maßnahmen: Kriminelle dürften es schwer haben, in einem abgesicherten Unternehmen Daten zu stehlen.

Zu den Basismaßnahmen der Prävention gehört des Weiteren die Verschlüsselung. Sie kann ein sehr wirksamer Schutz vor einem Missbrauch personenbezogener Daten sein, nämlich dann, wenn dem Angreifer trotz Zugriff auf die Daten verarbeitenden Systeme der Inhalt der Daten verwehrt bleibt. Ebenso wichtig ist die Zugriffskontrolle. Nahezu jeder Vorfall basiert auf kompromittierten Zugangsdaten. Multi-Faktor-Authentifizierung, Berechtigungsmanagement und Konzepte zur Verwaltung von Identitäten reduzieren nachweislich das Risiko erfolgreicher Angriffe.

In den Bereich der **reaktiven Sicherheit** fallen zunächst das Monitoring und die Angriffserkennung. Das frühzeitige Erkennen von Anomalien, ihre Qualifizierung und die zeitnahe Eindämmung laufender Angriffe in ihrer Frühphase sind für einen wirksamen Schutz und somit auch zur Vermeidung von Haftungsrisiken unverzichtbar geworden. Dafür sind sowohl passende Technologien (Next Generation SIEM; Endpoint Detection and Response (EDR), Network Detection and Response (NDR), Extended Detection and Response (XDR), Identity-Protection-Dienste, die bei Datenschutzverletzungen warnen) als auch Expertenteams notwendig, die rund um die Uhr Alarme qualifizieren, Vorfälle analysieren und die gezielte Eindämmung einleiten können.

Die wenigsten IT-Umgebungen sind darauf ausgelegt, im Falle eines Angriffs gute Werkzeuge zur Analyse, Eindämmung und zum Krisenmanagement bereitzustellen. Anders gesagt: Die Incident Response Readiness fehlt. Dabei ist oft alles vorhanden und muss nur für den Ernstfall optimiert werden, etwa redundante Kommunikationswege und offline verfügbare Ablaufpläne.

Mitarbeiter müssen geschult und vorbereitet sein

Ebenso wichtig wie die technische Seite sind die **organisatorischen Maßnahmen.** Mitarbeiter stellen nicht immer das größte, aber sicher das am schwierigsten handhabbare Risiko dar. Sensibilisierung und regelmäßige Schulungen mit unterschiedlichen Schwerpunkten können Fehlverhalten verhindern und den richtigen Umgang mit Ausnahmesituationen vermitteln.

Ein gut dokumentiertes Datenschutz- und Informationssicherheitsmanagementsystem zeigt, dass das Unternehmen Datenschutz ernst nimmt und Maßnahmen konsequent umsetzt. Vor Gericht sind diese Dokumentationen zukünftig Gold wert.

Der Umgang mit Sicherheitsvorfällen und Datenpannen darf nicht dem Zufall überlassen werden. Es gilt, klare Verantwortlichkeiten und Abläufe zu schaffen (Krisenpläne), verschiedene Szenarien zu berücksichtigen (Playbooks) und die Kommunikation mit Betroffenen, Behörden und den Umgang mit weiteren Stakeholdern im Vorfeld zu regeln (Krisenkommunikation, Rechtsberatung). Verteidigung funktioniert nur dann gut, wenn sie regelmäßig geübt wird. Insbesondere Informationssicherheitsvorfälle und Datenpannen stellen Organisationen vor so komplexe Herausforderungen, dass nur regelmäßiges Üben dazu führt, im Krisenfall fehlerfrei zu agieren.

Über die Abhängigkeit von Dienstleistern und Lieferanten, aber auch durch

die oft weitreichenden technischen Verbindungen und Zugriffsmöglichkeiten besteht heute auch ein hohes Risiko, Teil eines Datenschutzvorfalls zu werden, der gar nicht im eigenen Unternehmen begonnen hat. Die kritische Bewertung und Berücksichtigung von Lieferanten beim Risikomanagement rückt deshalb zunehmend in den Fokus.

Hilfe von außen

Kaum ein Unternehmen kann heute die enormen Anforderungen eines Sicherheitsvorfalls beziehungsweise einer Datenschutzpanne noch mit eigenen Ressourcen abdecken. Nicht nur kleine Unternehmen benötigen in der Regel **externe Unterstützung.** Auch für große Unternehmen ist die Zusammenarbeit mit externen Dienstleistern und Experten entscheidend. Diese sind 24/7 verfügbar, bieten stets aktuelles Know-how, können kurzfristig auf Bedrohungen reagieren und sind geübt in deren Analyse und Beseitigung.

Für kleinere Unternehmen ist es deutlich schwieriger, dieses Service-Level finanziell zu schultern. Hier bieten die Managed Services von EDR/XDR-Herstellern einen ersten Ansatz, bei der Angriffserkennung zu unterstützen und bei Vorfällen erste Maßnahmen einzuleiten.

Die Motivation für ausreichende Sicherheitsmaßnahmen sollte nicht nur in der Einhaltung gesetzlicher Pflichten bestehen. Es liegt auch unabhängig von jeglicher Vorgabe im ureigenen Interesse eines Unternehmens. Erfolgreiche Hackerangriffe sind nicht nur ein Problem der IT-Abteilung, sie führen in der Regel zu einer veritablen Krise des gesamten Unternehmens bis hin zur Insolvenz.

Fazit

Das Urteil des BGH ist ein Weckruf für Unternehmen. Mit ausreichenden technischen und organisatorischen Maßnahmen lassen sich nicht nur Schadensersatzklagen abwehren, sondern auch die Unternehmenswerte langfristig sichern. Cybersecurity ist dabei kein einmaliges Projekt, sondern eine kontinuierliche Aufgabe, die von der Geschäftsleitung aktiv unterstützt werden muss. (ur@ix.de)

Quellen

Das erwähnte EuGH-Urteil ist über ix.de/zvh3 zu finden.

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.

MAREK STIEFENHOFER

ist geschäftsführender Gesellschafter der r-tec IT Security GmbH und unterstützt seit über 20 Jahren Unternehmen dabei, sich auf Bedrohungen vorzubereiten und eine ganzheitliche Cybersecurity Readiness aufzubauen.