Folgenloser GAU

Kein Bußgeld für die Datenpanne bei Buchbinder

Zehn Terabyte sensibler Kundendaten der Autovermietung Buchbinder waren wochenlang für jedermann im Netz zugänglich. Rechtliche Konsequenzen hat dies für das Unternehmen nicht, wie die zuständige Datenschutzbehörde nun gänzlich unerwartet mitteilte.

Von Joerg Heidrich

Es war nicht irgendeine Sicherheitslücke: Teils höchst persönliche Daten von drei Millionen Kunden des Autovermieters Buchbinder standen Anfang 2020 wochenlang völlig ungeschützt zum Abruf bereit. Es ging um Informationen wie Adressen, Telefonnummern, Kontoverbindungen, aber auch detaillierte Unfallberichte, wie c't in einer gemeinsamen Recherche mit der Wochenzeitung Die Zeit herausgefunden hatte [1].

Die Ursache des Lecks lag in einem eher profanen Konfigurationsfehler eines externen Backup-Servers begründet: Über den offenen Port 445 hatten offensichtlich fahrlässig agierende Admins SMB-Zugriff gestattet und damit die Archive aus dem Internet einsehbar gemacht. Sämtliche Daten waren unverschlüsselt zu finden, ein Passwort für den Zugang war nicht erforderlich.

Gerade die nicht vorhandene Zugriffssicherung stellt nach Einschätzung aller von c't befragten Experten einen erheblichen Verstoß gegen die DSGVO dar. Als zuständige Aufsichtsbehörde für die Buchbinder-Gruppe hatte sich das Bayerische Landesamt für Datenschutzaufsicht mit Sitz in Ansbach der Sache angenommen. Für Erstaunen hatte die Behörde bereits früh mit der Einschätzung gesorgt, dass es sich bei der Datenpanne nicht um einen Fall nach Artikel 34 der DSGVO handelt.

Dieser Vorschrift zufolge hätte der Autovermieter alle betroffenen Kunden über die Datenpanne informieren müssen, sofern dadurch „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten" der Betroffenen entstanden wäre. Auf eine persönliche Unterrichtung zum mehr als schludrigen Umgang mit ihren Daten warten die Kunden, die bereits über die Medien von der Panne erfahren haben, bis heute.

Datenschutzexperten gingen außerdem davon aus, dass die Behörde ein hohes Bußgeld verhängen würde. Schließlich liegt ein recht eindeutiger Verstoß unter anderem gegen Artikel 32 DSGVO vor, der die technischen Anforderungen zum Schutz von Daten definiert. Immer wieder hakte c't bei der bayerischen Datenschutzaufsicht nach, um den Verfahrensstand zu erfragen. Im April schließlich teilte die Behörde mit, dass sie die Akte bereits im Dezember 2021 geschlossen hat.

„Angestiegene Sanktionsempfindlichkeit"

Es habe kein Anlass bestanden, „von Abhilfe- beziehungsweise Sanktionsbefugnissen Gebrauch zu machen". Maßgebliche Umstände seien dabei insbesondere „die Zurechenbarkeit des der Datenschutzverletzung zugrunde liegenden Fehlverhaltens und umfassende und effektive eigenverantwortliche Abhilfemaßnahmen sowie die pandemiebedingt angestiegene Sanktionsempfindlichkeit des Unternehmens" gewesen. Im Ergebnis kommt der Autovermieter für seine Datenpanne also ohne jegliche Sanktion durch die Behörde davon.

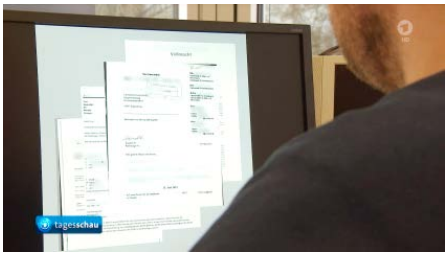

Bild: tagesschau.de

„Geringe Eintrittswahrscheinlichkeit"? Den Zugriff eines c't-Redakteurs auf die Buchbinder-Kundendaten hat beispielsweise die ARD-Tagesschau dokumentiert.

Die zugrunde liegende Argumentation dürfte selbst jene Juristen erstaunen, die das Datenschutzrecht sehr lax auslegen. Der Sachverhalt begründe, so die Behörde, grundsätzlich tatsächlich eine Verletzung von Artikel 32 der DSGVO. Sofern Daten ungeschützt im Netz liegen, geht die Behörde davon aus, „dass diese auch abgerufen wurden". In einem solchen Fall unterliege es dann dem Verantwortlichen – also der Buchbinder-Gruppe – nachzuweisen, dass dies nicht der Fall war, beispielsweise „durch die Auswertung von Log-Dateien samt übertragenen Datenmengen".

Kann der Betreiber des offenen Servers aber nachweisen, dass es nur eine „begrenzte, gegebenenfalls sogar individuell identifizierbare und damit spezifisch zu bewertende Anzahl von Akteuren" gab, die Zugriff auf die Daten gehabt haben, so sei das zu berücksichtigen. Durch Analysen des Netzwerkverkehrs habe Buchbinder „eine geringe Eintrittswahrscheinlichkeit eines Abrufs mit dem Zweck eines Datenmissbrauchs" ermittelt.

Zur Erinnerung: Sowohl c't- als auch Zeit-Redakteure sowie unser Tippgeber hatten mehrfach auf die Daten zugriffen, weshalb eine ganze Menge unterschiedlicher IP-Adressen in den Log-Dateien aufgetaucht sein dürften. Überdies könnten bei einem Angriff von Unbekannt die Log-Dateien nachträglich manipuliert worden sein.

Fabian Schmieder, Professor für Medienrecht und Datenschutz an der Hochschule Hannover, zeigte sich gegenüber c't erstaunt über die Entscheidung. Er kritisiert vor allem die Annahme der Behörde, dass es auf die Intention der Personen ankommen soll, die auf die Daten zugegriffen haben. Maßgeblich sei allein, dass durch die Fehlkonfiguration ein unberechtigter Zugriff faktisch ermöglicht wurde. Nach seiner Ansicht liegt ein schwerwiegender Verstoß gegen Artikel 32 Absatz 1 DSGVO vor, der ein Bußgeld rechtfertigen würde. *(hob@ct.de)* c't

Literatur

[1] Ronald Eikenberg, Hartmut Gieselmann, Joerg Heidrich, Christian Wölbert: Daten-GAU bei Buchbinder, Persönliche Informationen von 3 Millionen Kunden der Autovermietung Buchbinder offen im Netz, c't 4/2020, S. 12