Bild: Albert Hulm

Daten-GAU bei Buchbinder

Persönliche Informationen von 3 Millionen Kunden der Autovermietung Buchbinder offen im Netz

Es ist wohl eines der größten Datenlecks in der Geschichte der Bundesrepublik: Kundendaten der Autovermietung Buchbinder waren wochenlang für jedermann im Netz offen zugänglich, samt Adressen und Telefonnummern von Politikern, Unfallberichten …

Von Ronald Eikenberg, Hartmut Gieselmann, Joerg Heidrich und Christian Wölbert

Der Hinweis, der die c't-Redaktion vor Weihnachten erreichte, ließ nichts Gutes erahnen. „Bei unseren Überprüfungen sind wir auf Datenbanken einer der größten Autovermietungen Deutschlands aufmerksam geworden", schrieb uns Matthias Nehls, Chef der Flensburger IT-Sicherheitsfirma „Deutsche Gesellschaft für Cybersicherheit. Persönliche Daten von Millionen Kunden, Unfallberichte mit Informationen zu Alkoholfahrten, vertrauliche Mails und Anwaltsschreiben, unverschlüsselte Passwörter – all das stehe komplett ungeschützt im Netz.

Bei einem Treffen Anfang Januar zeigte sich schnell, dass er nicht übertrieben hatte: Als er auf seinem Laptop eine IP-Adresse im Windows-Explorer eingibt, erschienen sofort Ordner mit riesigen Backup-Dateien, teils über ein Terabyte groß. Ein Passwort oder ein Benutzername wurde nicht abgefragt. „Das ist eine offene SMB-Freigabe", erklärte Nehls.

Dort lag auch ein unverschlüsseltes Backup einer MSSQL-Datenbank der Autovermietung Buchbinder – mit Vornamen, Namen, Adressen, Geburtsdaten, Führerscheinnummern und weiteren Informationen von Abermillionen Kunden. Als einem Redakteur einfiel, dass sein Schwiegervater neulich bei Buchbinder gebucht hatte, fand sich sofort die entsprechende Zeile in der Datenbank.

Der IT-Experte berichtete, er habe den Datenschutzbeauftragten von Buchbinder bereits am 9. Dezember per E-Mail darüber informiert, dass seine Security-Firma auf „eine sehr massive Datenlücke" gestoßen sei, die „dringend" geschlossen werden müsse. Als Buchbinder

auch auf eine zweite Mail nicht reagierte, habe er sowohl den zuständigen Landesdatenschutzbeauftragen in Bayern als auch die Redaktionen von c't und DIE ZEIT informiert. Die beiden Redaktionen prüften dann gemeinsam die Größe und Bedeutung des Datenlecks.

Wer ist Buchbinder?

Buchbinder ist einer der größten deutschen Autovermieter und nach eigenen Angaben „Marktführer im Privatkundensegment PKW und LKW in Deutschland und Österreich". Die Unternehmensgruppe mit Hauptsitz in Regensburg beschäftigt mehr als 2500 Mitarbeiter und betreibt rund 165 Mietstationen in Europa. Die Kerngesellschaft der Buchbinder-Gruppe, die Charterline Fuhrpark Service GmbH in Regensburg, machte 2018 laut Jahresabschluss einen Umsatz von gut 350 Millionen Euro. Ihr zur Seite stehen laut Datenschutzerklärung die Carpartner Nord GmbH sowie die Terstappen Autovermietung GmbH in Duisburg. Seit 2017 gehört Buchbinder zum französischen Europcar-Konzern.

Eigentlich sollte man bei einem internationalen Konzern dieser Größe erwarten, dass er gewissenhaft mit seinen Firmen- und Kundendaten umgeht. Buchbinders IT-Abteilung legte immerhin tägliche Backups an und nutzt laut Who-is-Abfrage einen durch Charterline angemieteten Server bei der PlusServer GmbH in Köln. Auf diesem wurden jeden Wochentag .bak- und .log-Dateien gespeichert – insgesamt über zehn Terabyte. Auf dem Server war jedoch fatalerweise Port 445 offen, der Datenübertragungen per SMB (Server Message Block) erlaubt. Die Dateien waren jeweils mehrere hundert Gigabyte bis über ein Terabyte groß. Wer sie kopieren wollte, brauchte kein Passwort, sondern nur genügend große Festplatten und ein paar Stunden Zeit.

Millionen Betroffene

Die Backups enthielten über 5 Millionen Dateien mit umfangreicher Firmenkorrespondenz nebst eingescannten Rechnungen, Verträgen, Faxen, E-Mails und Schadensbildern von Autos. Zudem war dem Augenschein nach die komplette MSSQL-Firmendatenbank ohne Passwort gesichert. Sie umfasste laut den Analysen von c't und ZEIT über 9 Millionen Mietverträge, von heute bis zurück zum Jahr 2003. Neben den Mietern sind auch die Fahrer mit Name, Adresse, Geburtsdatum, Führerscheinnummer und -Ausstellungsdatum aufgeführt. Viele haben zudem Mobilfunknummern und E-Mail-Adressen angegeben. Kreditkartennummern fanden sich zwar nicht in der Datenbank, wohl aber Zahlungsinformationen und Bankverbindungen auf PDF-Scans von Rechnungen.

Von etwas über 3 Millionen Mietern der vergangenen 18 Jahre stammen rund 2,5 Millionen aus Deutschland, etwa 400.000 aus Österreich und die übrigen rund 114.000 aus Italien, der Slowakei und Ungarn. Ihnen zugeordnet sind 3,1 Millionen Fahrer aus aller Herren Länder.

Hinzu kommt eine Datenbank mit über 500.000 Unfällen, die bis ins Jahr 2006 zurückreichen. Erfasst wurden dort neben Informationen über die Fahrer der gemieteten Autos auch die Namen, Adressen und Kennzeichen von Unfallgegnern sowie eventueller Zeugen samt Telefonnummern. Vereinzelt fanden wir auch Namen und Kontaktdaten von Verletzten und tödlich Verunglückten. Neben Zeit und Ort war auch vermerkt, ob eine Blutprobe von der Polizei angeordnet wurde.

Mitarbeiter und Geschäftskunden wurden ebenfalls erfasst. Zudem fanden wir Login-Informationen von Angestellten und Nutzern der Online-Portale sowie dem Flottenmanagement von Buchbinder. Über 3000 von etwa 170.000 Passwörtern waren im Klartext gespeichert.

Authentische Daten

Dass die Datenbank authentisch ist, konnten wir anhand von 13 Mieter- und Fahrerdaten von Redakteuren und Angestellten bei Heise Medien verifizieren. Betroffen sind offenbar nicht nur Kunden, die direkt Fahrzeuge bei Buchbinder mieteten. Ein Redakteur der ZEIT fand seine Daten, weil er ein Fahrzeug über das Online-Portal billiger-mietwagen.de geordert hatte. Die Rechnung lautete auf Car Del Mar, einem Broker für Autovermietungen aus Hamburg. Buchbinder arbeitet offenbar mit vielen solchen Vermittlern und Vergleichsportalen zusammen, die dafür laut Firmendatenbank eine Provision erhalten. Kunden wissen am Ende mitunter gar nicht, dass ihr Fahrzeug von Buchbinder stammt und ihre Daten dort gespeichert sind. Organisiert werden Fahrzeugvermietungen oft über die Carpartner Nord GmbH. Über die Tochter Global Rent-a-Car vermietet Buchbinder zudem weltweit Fahrzeuge.

c't und DIE ZEIT informierten Buchbinder am 20. Januar über das Datenleck: „Sofort nach Kenntnisnahme des Sachverhalts haben wir unverzüglich die Schließung der entsprechenden Ports durch unseren mit der Betreuung und Absicherung der Server beauftragten Vertragspartner veranlasst", teilte uns die zur Buchbinder-Gruppe gehörende Terstappen Autovermietung GmbH schriftlich mit. Auf Fragen, wie lange das Datenleck bestand und wie viele Zugriffe es von außen gab, ging das Unternehmen ebenso wenig ein wie auf die Rechtsgrundlage, auf der Kunden- und Unfalldaten weit über zehn Jahre gespeichert wurden.

Kleiner Fehler, große Wirkung

Oft sind Konfigurationsfehler schuld, wenn Kundendaten im großen Stil im Netz landen. Bereits ein Klick an der falschen Stelle genügt – und schon ist das System auf der ganzen Welt erreichbar. Mitunter kann auch ein Bug im Router dazu führen – wie zuletzt bei einer Arztpraxis in Celle, wo Daten von 30.000 Patienten offen im Netz standen.

Stellt man einen Dienst ins Netz, ist es nur eine Frage von Minuten oder höchstens Stunden, bis das jemandem auffällt und Zugriffsversuche starten. Wenn ein Datendieb wie bei Buchbinder dabei keinerlei Schutzmechanismen umgehen muss, handelt es sich dabei im juristischen Sinne nicht einmal um einen „Hackerangriff".

Um solch exponierte Systeme aufzuspüren, ist keine Handarbeit nötig: Open-Source-Tools wie der Netzwerkscanner ZMap klopfen in weniger als einer Stunde sämtliche IPv4-Adressen auf offene Dienste ab. Sicherheitsexperten finden damit schnell heraus, wo etwa der Port 445 für SMB-Dateifreigaben offen ist.

Die Deutsche Gesellschaft für Cybersicherheit war auf den offenen Port bei einem ihrer Routine-Scans gestoßen. Die Firma unterhält eine Online-Datenbank namens Cyberscan.io, die Firmen bei der Abdichtung eventueller Sicherheitslöcher helfen soll. Die SMB-Freigabe von Buchbinder war aber nicht nur dort gelistet. Die auf Sicherheitslücken spezialisierte Suchmaschine Shodan.io zeigte den Rechner ebenfalls an – zusammen mit 125 weiteren Servern mit ungeschützten SMB-Freigaben für Backups in Deutschland.

Für Neugierige war der Buchbinder-Server also relativ leicht zu entdecken. Jeder, der wusste, wo er nachzuschauen hatte, konnte sich frei daran bedienen. Für den Download genügte der Windows-Datei-Explorer.

SMB-Sperren

Weil ein offener SMB-Port so fatale Folgen haben kann, sperren viele Internet-Provider per se Zugriffe auf Port 445. Neben Zugriffen auf ungesicherte Dateiserver drohen nämlich auch Hackerattacken. So nutzte etwa auch der WannaCry-Schädling, der im Jahr 2017 weltweit hunderttausende Systeme infizierte, eine Schwachstelle im SMB-Protokoll aus.

Die Port-Blockade erschwert es, zu überprüfen, ob hinter der eigenen IP-Adresse ein offener Dienst läuft, der da nichts zu suchen hat. Wer den eigenen Anschluss oder das Unternehmensnetz untersuchen möchte, muss deshalb einen Portscan aus einem anderen Netz starten, das Zugriffe auf SMB-Dienste grundsätzlich erlaubt. Der einfachste Weg ist der Netzwerkcheck von heise Security (siehe ct.de/yyak). Nach einem Klick auf „Scan starten“ überprüft der Komplett-Check, über welche Ports die eigene IP-Adresse aus dem Internet erreichbar ist.

Wer andere IP-Adressen überprüfen möchte, kann dazu den Netzwerkscanner nmap (siehe ct.de/yyak) nutzen, der auch hinter den Kulissen des Netzwerkchecks zum Einsatz kommt. Das Kommandozeilen-Tool läuft unter allen Desktop-Betriebssystemen und wird im einfachsten Fall mit *nmap IP-Adresse* aufgerufen.

Lohnenswert ist auch ein Blick auf die Shodan-Ergebnisse zu den jeweiligen IP-Adressen. Geben Sie die IP-Adresse hierzu auf shodan.io ein und starten Sie die Suche. Wer es genau wissen will, kann den Dienst des Buchbinder-Leck-Entdeckers Cyberscan.io nutzen. Dieser spürt nicht nur offene Dienste auf, sondern gibt auch Hinweise auf weitere mögliche Sicherheitsprobleme.

Angriffspotenziale

Die bei Buchbinder geleakten Daten sind für Cyber-Schurken enorm wertvoll. Es handelt sich um valide Informationen von Millionen Bürgern – einschließlich Name, Firmenzugehörigkeit, Anschrift, Geburtsdatum, Telefon- und Führerscheinnummer. Im Unterschied zu Daten, die Nutzer etwa für die Teilnahme an einem Gewinnspiel angeben, müssen die bei Buchbinder hinterlegten Daten echt sein, damit es zum Abschluss eines gültigen Mietvertrags kommen kann.

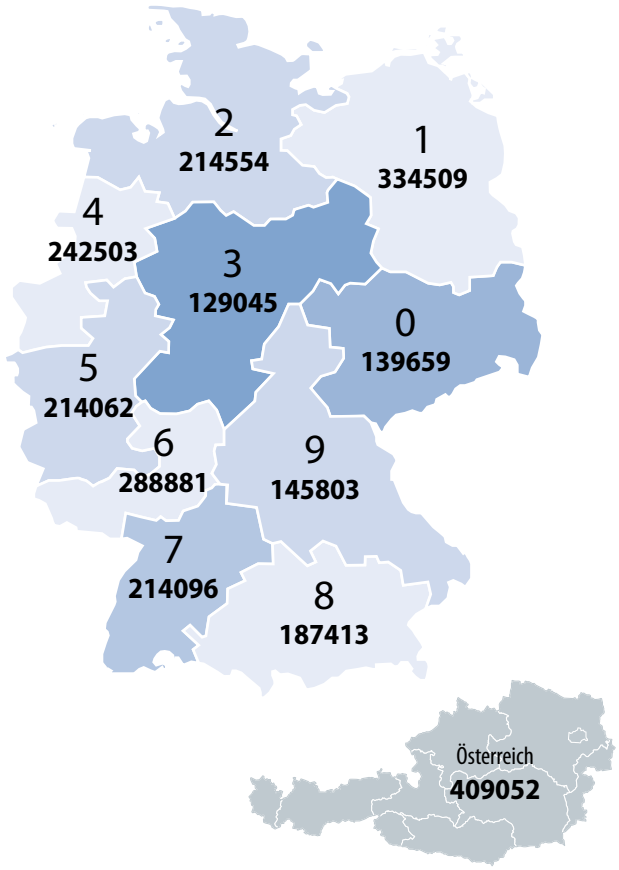
Den größten Schaden hat gewiss Buchbinder: Die Kundendaten gehören zu den größten Schätzen eines Unternehmens, die Datenbank wurde über mehr als ein Jahrzehnt aufgebaut. Wer jetzt alles darauf Zugriff hatte, lässt sich nicht mehr nachvollziehen. Mitbewerber könnten unbezahlbare Einblicke in die Flotte des Unternehmens erhalten haben. Der Leak dürfte auch zu einem erheblichen Vertrauensverlust seitens der Kunden führen – ganz zu schweigen von etwaigen DSGVO-Bußgeldern und eventuellen Schadenersatzforderungen.

Die erbeuteten Daten könnten sich auf verschiedene Arten missbrauchen lassen. Zunächst geht es ums große Geld: Ein Angreifer könnte etwa gezielt nach Mietvorgängen von Unternehmenskunden suchen, um die persönlichen Kontaktdaten der involvierten Mitarbeiter herauszusuchen. Anschließend könnte er diese Daten nutzen, um im Namen des Mitarbeiters mit dessen Arbeitgeber zu kommunizieren, um sich Vertrauen zu erschleichen und sich weiter vorzuarbeiten.

Denkbar wäre auch ein groß angelegter Phishing-Angriff auf Buchbinder-Kunden: Der Täter könnte Phishing-Mails verschicken, die dazu auffordern, die bei der Autovermietung hinterlegten Kreditkartendaten zu aktualisieren. Er könnte vorgeben, dass

Regionale Verteilung nach PLZ

Rund 2,5 Millionen Kunden von Buchbinder verteilen sich über das gesamte Bundesgebiet. Hinzu kommen rund 409.000 Kunden aus Österreich und knapp 114.000 aus dem übrigen Ausland.



es bei einer Abbuchung zu einem Problem gekommen ist und sich dabei sogar konkret auf eine Vermietung beziehen. Für die Empfänger wäre eine solche Mail kaum von einer echten zu unterscheiden.

Brisante Kunden

Spam, Phishing, Einkäufe im fremden Namen oder anderer Identitätsklau stehen erst am Ende der Verwertungskette und könnten noch Jahre später eintreten, wenn der Vorfall längst vergessen ist. Dazu ließe sich die Datenbank etwa in kleinere Häppchen aufteilen. Da viele Kunden einen Wagen auf Geschäftskosten mieten, lassen sich einzelne Personen leicht verschiedenen Firmen, Vereinen und Parteien zuordnen.

Unter den Kunden findet man beispielsweise zahlreiche Prominente aus Sport und Unterhaltung, Spitzenpolitiker von CSU und AfD sowie Robert Habeck von den Grünen – mit Privatadresse, Handynummer und E-Mail-Adresse. Darüber hinaus sind mehrere hundert Angehörige verschiedener Botschaften gelistet – nicht nur aus Deutschland und Österreich, sondern auch aus den USA, Russland, China, dem Libanon, Israel, dem Iran, Saudi-Arabien oder auch Nord-Korea.

Dutzende Einträge führen zu Mitarbeitern verschiedener Bundesministerien, darunter ein ehemaliger hochrangiger Beamter des Verfassungsschutzes. Zu den Betroffenen zählt unter anderem auch der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Arne Schönbohm. Gegenüber den Kollegen von der ZEIT erklärte er: „Der Fall zeigt leider, dass auch sehr sensible personenbezogene Daten immer wieder nur unzureichend geschützt werden. Egal ob ich – wie in diesem Fall – persönlich betroffen bin oder nicht, solche Fälle ärgern mich sehr, weil sie vermeidbar wären."

Betroffen sind auch Mitarbeiter der Polizei und der Bundeswehr. Aus Österreich hatte 2008 sogar ein Mitglied des „Einsatzkommando Cobra Süd" einen Wagen gemietet, eine Art Pendant zur GSG 9 in Deutschland. Aus Deutschland findet man beispielsweise zwei Mitarbeiter von FinFisher, einem öffentlichkeitsscheuen Hersteller von Spionage-Software.

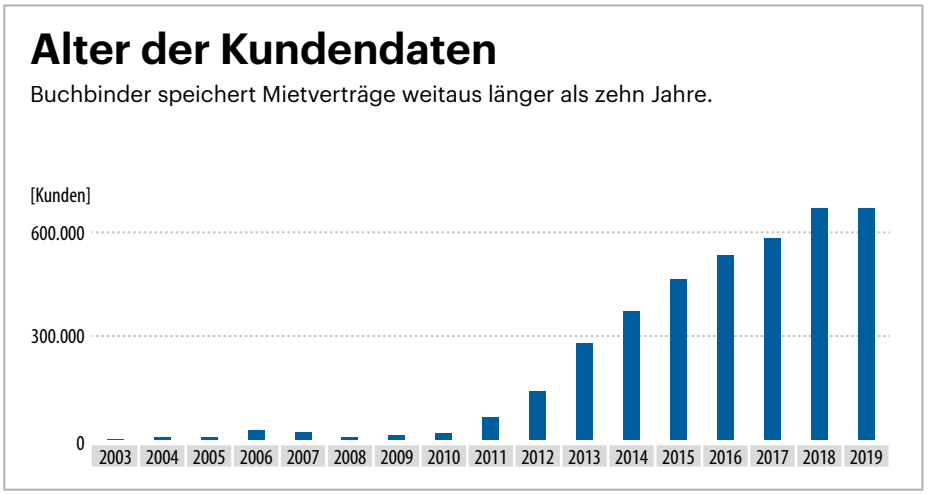
DSGVO-Verstöße

Aus juristischer Sicht ist ein derart offener Server ein geradezu katastrophaler Verstoß gegen die Vorgaben der DSGVO. Art. 32 stellt hier sehr hohe Anforderungen an die IT-Sicherheit. Dabei ist ein für die Sensibilität der jeweiligen Informationen angemessenes Gesamtkonzept festzulegen, umzusetzen und zu dokumentieren. Die dafür zwingend notwendige Risikobewertung ist aus dem Blickwinkel der einzelnen Kunden und Mitarbeiter zu treffen – nicht aus der des Unternehmens. Es kommt also nicht darauf an, welche Schäden ein Unternehmen durch eine Datenpanne treffen könnten. Entscheidend ist vielmehr, was den Inhabern der Daten drohen könnte, etwa durch den Abfluss sensibler Kranken- oder Zahlungsinformationen.

Sollten die zuständigen Aufsichtsbehörden einen Verstoß gegen die DSGVO feststellen, wäre ein sehr hohes Bußgeld fällig. In Berlin wurde Ende 2019 ein Bußgeld in Höhe von 14,5 Millionen Euro gegen eine Immobiliengesellschaft verhängt. Vorgeworfen wurde der Deutschen Wohnen unter anderem das Vorhalten von Datensätzen, für deren Erfassung und maximal erlaubte Speicherdauer es keine Rechtsgrundlagen gibt.

Hauptausgangspunkt für die Berechnung ist der Jahresumsatz des Unternehmens. Auf dessen Basis ergibt sich ein Tagessatz, der je nach Schweregrad und Verschulden zu vervielfachen ist. Entscheidend wird im Buchbinder-Fall deshalb sein, wie das Leck zustande kam und wer dafür verantwortlich ist.

Zumindest auf der Website präsentieren sich die drei Unternehmen der Buchbinder-Gruppe im Rahmen der Datenschutzerklärung als gemeinsam Verantwortliche im Sinne der DSGVO. Darüber hinaus gelten die DSGVO-Pflichten uneingeschränkt auch für Dienstleister, die der für die Daten Verantwortliche zu Auftragsverarbeitungen heranzieht. Buchbinder könnte sich also nicht damit rausreden, der Unfall sei allein die Schuld eines Dienstleisters.



Erschwerend kann im vorliegenden Fall sein, wenn besonders sensible personenbezogenen Daten im Sinne von Art. 9 DSGVO betroffen sind, die noch stärker geschützt werden müssen. In der Buchbinder-Datenbank lassen sich beispielsweise Kunden politisch, religiös, nach sexuellen Vorlieben oder Erkrankungen zuordnen. So findet man Fahrten von Kreis- und Landesverbänden aller im Bundestag vertretenen Parteien, wie auch der DKP und NPD. Gelistet sind mehrere Hundert islamische Vereine, Einträge jüdischer Gemeinden wie auch Schwulen- und Lesben-Vereine sowie Selbsthilfegruppen von Süchtigen.

Was Betroffene tun können

Art. 34 DSGVO sieht vor, dass im Falle eines Sicherheitslecks die Betroffenen von der Verletzung zu informieren sind, also Kunden, Mitarbeiter und Geschäftspartner von Buchbinder. Voraussetzung dafür ist, dass durch den Vorfall „voraussichtlich ein hohes Risiko" für deren persönliche Rechte und Freiheiten entsteht, wofür einiges spricht.

Wer wissen will, ob seine Informationen in der Datenbank gespeichert und von dem Leck betroffen sind, kann dies bei Buchbinder erfragen. Art. 15 DSGVO bietet allen Bürgern die Möglichkeit, von dem Unternehmen eine Selbstauskunft zu verlangen. Wir haben für eine solche Anfrage ein Formular vorbereitet, das Sie an die Charterline Fuhrpark Service GmbH, Kulmbacher Str. 8.10, 93057 Regensburg adressieren und per E-Mail an datenschutz@buchbinder.de schicken können. Die für private Zwecke kostenlos verwendbare Vorlage ist unter ct.de/yyak abrufbar. *(hag@ct.de)* c't

Formulare und Tools: ***ct.de/yyak***