Augsburger Verkehrs- und Tarifverbund

FAQ zum Hackerangriff auf AVV-Kundenportal im September 2020
(Stand: 13. Oktober 2020)

1. Was ist über den Hackerangriff bekannt?

Eine anonyme Hackergruppe hatte im September 2020 Zugriff auf eine Datenbank des Augsburger Verkehrs- und Tarifverbunds (AVV). Möglicherweise betroffen sind Datensätze, die von Kunden des AVV bei Bestellung einer Kundenkarte erhoben wurden. Auf der Datenbank befanden sich etwa 156.000 Kundendatensätze. Der AVV bedauert diesen Vorfall und die möglicherweise daraus entstandenen Unannehmlichkeiten für Kunden außerordentlich. Die Hackergruppe hat nach eigener Aussage eine Sicherheitslücke genutzt, um auf die Daten zuzugreifen. Nach Aussagen der Hackergruppe gegenüber der Presse sei es ihnen bei dem Datenzugriff um die Vermeidung von Schäden bei Privatpersonen gegangen. Die Hackergruppe hat sich in der Presse von betrügerischen Aktivitäten distanziert. Der AVV konnte die ermittelten Sicherheitslücken am betroffenen Kundenkartensystem schließen. Die weitere Aufklärung ist Gegenstand laufender interner und behördlicher Ermittlungen.

2. Welche Daten befanden sich auf der Datenbank?

Auf der in Frage stehenden Datenbank befinden sich folgende Datensätze: Name, Anschrift, Geburtsdatum, Geschlecht, Telefonnummer (soweit bei Bestellung einer Kundenkarte angegeben), E-Mail-Adresse (soweit bei Bestellung einer Kundenkarte angegeben), Student (ja/nein bzw. Inhaberschaft einer campus-Karte), gewünschte Verbindung für die Kundenkarte (Start-, ggf. Umstieg- und Zielhaltestelle), bevorzugtes Beförderungsmittel (soweit bei Bestellung einer Kundenkarte angegeben; abstrakte Auswahlmöglichkeit Regionalbus, Regionalbahn oder Stadtwerke). Die Information über die gewünschte Verbindung der Kundenkarte ist lediglich für die Berechnung des Tarifs erforderlich. Konkrete Einzelfahrten oder eine Live-Lokalisierung lassen sich daraus nicht ableiten. Andere sensible Informationen, wie beispielsweise Passwörter oder Bankdaten, sind nicht auf der betroffenen Datenbank gespeichert.

3. Sind meine Daten betroffen?

Auf der Datenbank befanden sich Daten von Kunden des AVV, die eine Kundenkarte bezogen haben. Eine solche Kundenkarte kann etwa auch von Schülern, Auszubildenden, Praktikanten, Beamtenanwärtern oder Teilnehmern eines sozialen Jahres beantragt werden. Daten anderer Kunden des AVV (etwa Abo-Kunden) befanden sich nicht auf der Datenbank. Auch Informationen zu Nahverkehrskunden von AVV-Partnern, etwa den Augsburger Stadtwerken, DB Regio AG oder der Bayerischen Regiobahn, wurden auf der Datenbank nicht gespeichert.

4. Was muss ich jetzt tun?

Auch wenn wir keine Anhaltspunkte dafür haben, dass Ihre Daten für missbräuchliche Zwecke verwendet wurden bzw. werden, bitten wir Sie um erhöhte Aufmerksamkeit, insbesondere beim Öffnen verdächtigter E-Mails. Bitte öffnen Sie insbesondere keine Links oder Dateianhänge in verdächtigten E-Mails und/oder von unbekannten Absendern. Wir weisen vorsorglich darauf hin, dass der AVV per E-Mail weder Passwörter noch Bankverbindungen abfragt.

5. Welche Konsequenzen drohen mir, sollten meine Daten unbefugt verwendet werden?

Auch wenn wir keine Anhaltspunkte für eine missbräuchliche Verwendung der betroffenen Datensätze haben, möchten wir Sie vorsorglich auf Risiken hinweisen, die bei einer Offenlegung von Kontaktdaten allgemein bestehen können:

– Phishing-E-Mails, d.h. E-Mails, bei denen unter Vortäuschung eines falschen Sachverhalts Passwörter oder andere persönliche Informationen abgefragt werden;

– SPAM-E-Mails, d.h. unerwünschte E-Mails;

– E-Mails mit Schadsoftware, etwa versteckt in einem Anhang oder einem Link in einer E-Mail.

Weitere Informationen zu derartigen Risiken sowie möglichen Schutzmaßnahmen finden Sie auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI), abrufbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/risiken_node.html.

6. Welche Maßnahmen hat der AVV ergriffen?

Wir nehmen den Vorfall sehr ernst. Der AVV hat die ermittelten Sicherheitslücken am betroffenen Kundenkartensystem geschlossen und zusätzlich umfangreiche Maßnahmen ergriffen, um den Schutz personenbezogener Daten weiter zu erhöhen. Die Kundendaten wurden nach Bekanntwerden des Vorfalls umgehend auf eine neue, aktualisierte Server-Datenbank übertragen. Für die technische Aufarbeitung haben wir externe Experten eingebunden. Der AVV steht in engem Kontakt mit den zuständigen Polizei- und Datenschutzbehörden. Zudem führen wir umfangreiche präventive Maßnahmen zur Gefahrenabwehr an sämtlichen AVV-Online-Systemen durch, um den Schutz Ihrer Daten weiter zu erhöhen.

7. Wurden die zuständigen Behörden rechtzeitig informiert?

Ja. Wir haben umgehend die für uns zuständige Datenschutzbehörde über den Vorfall informiert. Daneben wurden das Landesamt für Sicherheit in der Informationstechnik (LSI), die Zentrale Ansprechstelle Cybercrime (ZAC), die Kriminalpolizei Augsburg sowie das Landeskriminalamt Bayern in den Vorfall eingebunden.

8. Warum wurde der Sicherheitsvorfall nicht sofort öffentlich gemacht?

Wir nehmen den Schutz Ihrer Daten sehr ernst. Die Abwehr möglicher Gefahren sowie die dazu erforderliche Aufklärung des Sachverhaltes hatten bzw. haben für uns oberste Priorität. Aufgrund forensischer Untersuchungen an den möglicherweise betroffenen Altsystemen, weiteren Absicherungsmaßnahmen an der neuen Datenbank sowie aus ermittlungstaktischen Gründen der Strafverfolgungsbehörden waren wir angehalten, zunächst keine Details zu dem Sicherheitsvorfall zu veröffentlichen.

9. Was weiß man über die Hacker?

Wir haben bislang keine Anhaltspunkte dafür, dass die Hacker betrügerische Absichten verfolgen. Nach Presseberichten handelt es sich um eine Hackergruppierung, die nach eigener Aussage auf Sicherheitslücken hinweisen wollte.

10. An wen kann ich mich bei Rückfragen wenden?

Für Ihre Rückfragen stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung:

– Per Postanschrift: Augsburger Verkehrs- und Tarifverbund GmbH, Datenschutzbeauftragter, Prinzregentenstraße 2, 86150 Augsburg

– Per E-Mail: datenschutz@avv-augsburg.de.

Über die Kontaktdaten können Sie auch unseren Datenschutzbeauftragten erreichen. Bitte beachten Sie, dass Daten im Internet allgemein nicht immer sicher übertragen werden können. Wir bitten Sie, keine sensiblen Daten per E-Mail an uns zu übermitteln. Wir bitten um Ihr Verständnis, dass wir Ihnen am Telefon und per E-Mail keine Auskunft über personenbezogene Informationen geben können.