Abgeordnetenhaus BERLIN

Drucksache 19 / 22 684
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

der Abgeordneten Gollaleh Ahmadi und Antje Kapek (GRÜNE)

vom 23. Mai 2025 (Eingang beim Abgeordnetenhaus am 23. Mai 2025)

zum Thema:

Cyberangriff auf die BVG – wie (un-)sicher sind unsere Verkehrsnetze?

und **Antwort** vom 3. Juni 2025 (Eingang beim Abgeordnetenhaus am 5. Juni 2025)

Senatsverwaltung für Wirtschaft,
Energie und Betriebe

Frau Abgeordnete Gollaleh Ahmadi (Bündnis 90/Die Grünen) und
Frau Abgeordnete Antje Kapek (Bündnis 90/Die Grünen)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei – G Sen –

Antwort
auf die Schriftliche Anfrage Nr. 19/22684
vom 23.05.2025
über Cyberangriff auf die BVG – wie (un-)sicher sind unsere Verkehrsnetze?

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Vorbemerkung der Verwaltung:
Die Schriftliche Anfrage betrifft Sachverhalte, die der Senat nicht in eigener Zuständigkeit und Kenntnis beantworten kann. Er ist gleichwohl bemüht, Ihnen eine Antwort auf Ihre Anfrage zukommen zu lassen und hat daher die Berliner Verkehrsbetriebe Anstalt öffentlichen Rechts (BVG) und die Berliner Beauftragte für Datenschutz und Informationssicherheit um Stellungnahme gebeten, die von dort in eigener Verantwortung erstellt und dem Senat übermittelt wurden. Sie werden nachfolgend wiedergegeben.

Vorbemerkung der BVG:
Bei dem Datenschutzvorfall handelt es sich nicht um einen „Hackerangriff“ gegen die BVG, sondern um einen IT-Angriff auf einen beauftragten externen Dienstleister. Systeme der BVG waren nicht betroffen. Bei dem Dienstleister handelt es sich um ein Unternehmen, das die BVG beim professionellen Massenversand von Vertriebsschreiben unterstützt. Alle Informationen zum Vorfall sind auf der Website der BVG zu finden.

1. Inwiefern wurden die Vorgaben des NIS2UmsuCG innerhalb der BVG umgesetzt? Insbesondere im Hinblick auf die Anforderungen an die Lieferkette und von Drittanbietern. Welche Ergebnisse hat eine Analyse und Risikobewertung der Lieferkettensicherheit ergeben?

Zu 1.: Die BVG hat nach eigener Auskunft im Zuge des Inkrafttretens des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) eine umfassende Betroffenheitsanalyse durchgeführt. Diese ergab, dass die BVG als Betreiber kritischer Infrastruktur im Sektor „Transport und Verkehr“ unter die erweiterten Pflichten des Gesetzes fällt. Ein besonderer Schwerpunkt liegt auf der Einbindung von Dienstleistern und Drittanbietern. Die Anforderungen der NIS2-Verordnung wurden in aktuellen Vertragswerken der BVG explizit berücksichtigt und in die funktionalen Leistungsbeschreibungen bei Vergabeverfahren aufgenommen.

2. Wie viele Schadensersatzbegehren nach Art. 82 Absatz 1 DSGVO sind bei der BVG bzw. bei dem Auftragsverarbeiter im Zuge des Kontrollverlusts über personenbezogene Daten eingegangen? Inwieweit ist eine rechtliche Prüfung durch die BVG für Schadensersatzansprüche im konkreten Schadensfall erfolgt und wie ist die rechtliche Auffassung der BVG zur Leistung von Schadensersatz im konkreten Schadensfall bei Berücksichtigung der jüngsten EuGH bzw. BGH Rechtsprechung?

Zu 2.: Die BVG teilt mit, dass bis zum Zeitpunkt der Beantwortung der Anfrage bei der BVG insgesamt 145 Schadensersatzbegehren im Zusammenhang mit dem Vorfall eingegangen sind. Darüber hinaus wurden eine sehr geringe Anzahl an Forderungen und Anfragen direkt gegenüber dem betreffenden Auftragsverarbeiter geltend gemacht. Jede der eingegangenen Forderungen wurde bzw. wird durch die zuständigen Fachbereiche in Zusammenarbeit mit der Rechtsabteilung der BVG individuell geprüft. Dabei erfolgt eine Einzelfallbewertung unter Berücksichtigung des tatsächlichen Schadenssachverhalts, der Art der betroffenen Daten sowie des geltend gemachten immateriellen Schadens. Ziel ist es, berechtigte Ansprüche zügig zu erkennen, unbegründete Forderungen jedoch ebenso rechtskonform zurückzuweisen.

Nach Auffassung der BVG verdeutlichen die Entscheidungen des Europäischen Gerichtshofs (Urteil vom 4. Oktober 2024, C-200/23) und des Bundesgerichtshofs (Urteil vom 11. Februar 2025, VI ZR 365/22), dass bereits ein „Kontrollverlust“ über personenbezogene Daten – unabhängig von einem konkreten Missbrauch – einen ersatzfähigen immateriellen Schaden darstellen kann, sofern eine tatsächliche individuelle Beeinträchtigung vorliegt. Im konkreten Vorfall betrafen die offengelegten Daten ausschließlich Informationen des allgemeinen Identitätsbereichs (Name, Vorname, Adresse, E-Mail-Adresse, Abonummer). Besondere Kategorien personenbezogener Daten im Sinne des Artikel 9 der Datenschutzgrundverordnung (DSGVO) waren nicht betroffen. Auch liegen der BVG bisher keine Nachweise über tatsächliche oder versuchte Missbrauchshandlungen im Zusammenhang mit dem Vorfall vor.

3. Welche Fragen sind der BVG von Seiten der BlnBDI gestellt worden, deren Beantwortungsfrist am 21.05.2025 ausgelaufen ist, wie im Ausschuss vom selbigen Tag berichtet. Wie schätzt die BlnBDI die Qualität der Beantwortung, Bereitschaft zur Transparenz sowie das Ausmaß der Betroffenheit personenbezogener Daten ein?

Zu 3.: Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) teilt hierzu mit: „Zu der Datenpanne kam es bei einem beauftragten Dienstleister der BVG. Dort hatte man bereits am 8. April 2025 Kenntnis von der Datenpanne. Die BlnBDI hat die BVG gebeten, zu begründen, warum die Datenpannenmeldung nicht binnen 72 Stunden nach Kenntnisnahme beim Dienstleister erfolgte. Die BlnBDI hat die BVG weiter um Vollzugsmeldung gebeten, sobald die Benachrichtigung der betroffenen Personen über die Datenpannenmeldung erfolgt ist, und die Übersendung eines anonymisierten Beispielsschreibens erbeten. Die BVG hat fristgerecht geantwortet. Mit diesen Antworten als Grundlage erfolgt die Sachverhaltsaufklärung anhand weiterer Nachfragen. Die BVG hat neben der schriftlichen Stellungnahme angeboten, auch über weitere Entwicklungen und wesentliche Erkenntnisse zu den Abläufen zu berichten und Transparenz sowie Kooperationsbereitschaft signalisiert. Die BlnBDI schätzt die Qualität der Beantwortung und die Bereitschaft zur Transparenz daher bisher als gut ein. Es handelt sich um eine hohe Anzahl der von der Datenpanne betroffenen Personen. Laut der BVG betrifft die Datenpanne keine Bankverbindungen oder Passwortinformationen. Hinsichtlich der betroffenen personenbezogenen Daten sind jedoch u. a. Identitätsdiebstähle und Phishing-Versuche auf Basis der offengelegten Daten wie Name, Kontaktdaten und Abo-Nummern nicht auszuschließen.“

Die BVG teilt ergänzend mit, dass sie weiterhin im Austausch mit der BlnBDI und anderen relevanten Stellen steht, um Transparenz und Datenschutzkonformität auch künftig zu gewährleisten.

4. Wie begründet die BVG die widersprüchliche Aussage in dem Schreiben an die Betroffenen eines möglichen Verlusts von personenbezogenen Daten die Möglichkeit zur vorsorglichen Änderung des Passworts, wenn doch keine Passwortdaten abgeflossen sind?

Zu 4.: Die BVG teilt mit, dass eine Passwortänderung im Zusammenhang mit dem Datenschutzvorfall weiterhin nicht erforderlich ist. Es handelt sich hierbei um eine empfohlene Vorsichtsmaßnahme und steht deshalb nicht im Widerspruch zu den Angaben im Schreiben.

5. Wie viel Zeit ist vergangen zwischen dem Bekanntwerden des Schadensfalls bei dem Auftragsverarbeiter und dem Ergreifen von Gegenmaßnahmen, die ausweislich des Schreibens an die Betroffenen unmittelbar eingeleitet worden sind? Welche konkreten Gegenmaßnahmen sind ergriffen worden? Bitte um konkrete Darstellung.

Zu 5.: Die BVG teilt mit, dass sie gesicherte Kenntnis über Art und Umfang der BVG-Betroffenheit am 30. April 2025 erlangte. Am 17. April 2025 ging beim zentralen Funktionspostfach (datenschutz@bvg.de) eine erste Mitteilung des Auftragsverarbeiters über einen potenziellen Sicherheitsvorfall ein. Zu diesem Zeitpunkt lagen lediglich allgemeine Hinweise auf einen möglichen unbefugten Zugriff vor – ohne gesicherte Informationen darüber, ob und in welchem Umfang Daten der BVG betroffen waren. Der

Zeitraum zwischen dem 17. und dem 30. April 2025 wurde nach Auskunft der BVG genutzt, um in mehreren Abstimmungsgesprächen mit dem Auftragsverarbeiter konkrete Informationen zum Vorfall zu erhalten. Die Meldung an die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) erfolgte unmittelbar nach der gesicherten Kenntnis der BVG-Betroffenheit am 30. April 2025.

Nach Aussagen der BVG wurden parallel zur Aufklärung des Sachverhalts erste Gegenmaßnahmen eingeleitet, insbesondere:

- Technische Überprüfung der BVG-Systeme, um eine etwaige Kompromittierung auszuschließen – mit negativem Befund;
- Dokumentation und Bewertung des Risikos für die betroffenen Personen auf Basis der verfügbaren Informationen;
- Interne Risikoanalyse und rechtliche Prüfung, insbesondere im Hinblick auf Meldepflichten gemäß Art. 33 und 34 DSGVO;
- Vorbereitung des Informationsschreibens an die betroffenen Personen;
- Empfehlungen zur Passwortänderung, Hinweise zur Erkennung von Phishing-Versuchen sowie allgemeine Sicherheitsinformationen, die mit dem Informationsschreiben kommuniziert wurden.

6. Wie viele personenbezogene Datensätze waren vom Vorfall konkret betroffen? Inwiefern konnte die BVG alle betroffenen Personen nachweislich kontaktieren? Auf welcher Grundlage wird angenommen, dass der Kreis der Betroffenen nicht über das bislang bekannte Maß hinausgeht? Sind mittlerweile widerrechtliche Nutzungen der Daten bekannt geworden?

Zu 6.: Die BVG teilt mit, dass durch den IT-Angriff auf den externen Dienstleister eine Datei mit 182.295 Kundendatensätzen betroffen ist. Es handelt sich um endgültig bestätigte Werte. Betroffen können nur diejenigen Personen sein, die im Zusammenhang mit dem Tarifprodukt „Berlin Abo“ von der BVG postalisch kontaktiert oder informiert wurden. Aktuell liegen der BVG keine Hinweise auf einen Missbrauch dieser Daten vor.

7. Welche konkreten Kategorien personenbezogener Daten wurden durch den Angriff kompromittiert? Inwieweit wurden die betroffenen Personen über den Umfang der abgeflossenen Daten informiert, und welche konkreten Schutzmaßnahmen wurden ihnen zur Abmilderung potenzieller Risiken empfohlen?

Zu 7.: Die BVG teilt mit, dass nach aktuellem Kenntnisstand die folgenden Daten von dem Datenschutzvorfall betroffen sind:

- Name,
- Postanschrift,
- E-Mail-Adresse, sofern angegeben,
- Kundennummer,

• Vertragsnummer Berlin-Abo.

Kontodaten und Passwörter sind nach Angaben der BVG nicht betroffen. Bei den betroffenen Daten handelt es sich um keine sensiblen Daten nach Artikel 9 DSGVO. Aktuell liegen der BVG keine Hinweise auf einen Missbrauch dieser Daten vor. Mit dem Informationsschreiben sowie auf der Website hat die BVG ihren Kundinnen und Kunden empfohlen, auf ungewöhnliche Aktivitäten und Nachrichten (insbesondere Phishing-E-Mails) im persönlichen E-Mail-Postfach zu achten. Auch wenn keine Passwortdaten abgeflossen sind, hat die BVG in Bezugnahme auf die Empfehlungen von Sicherheitsexperten bei einem Datenvorfall darauf hingewiesen, Passwörter vorsorglich zu ändern.

8. Besteht aus technischer Sicht die Möglichkeit, dass über bestehende Schnittstellen auch ein Zugriff auf das Kernsystem der BVG erfolgt sein könnte? Welche Maßnahmen wurden getroffen, um einen solchen Zugriff auszuschließen bzw. zu überprüfen?

Zu 8.: Die BVG teilt mit, dass die Datensätze über einen SFPT-Server des externen Dienstleisters übermittelt wurden, der sich in dessen Geschäftsräumen befindet. Die Datenübertragung war nur von der BVG mit Zugangsdaten des Dienstleisters möglich. Dadurch ist es nach Auskunft der BVG nahezu ausgeschlossen, dass BVG-Zugangsdaten abgeflossen sind oder Angreifer Zugang zur IT der BVG bekommen haben.

9. In welchem Umfang hat der Ausfall des beauftragten IT-Dienstleisters die Funktionsfähigkeit zentraler Betriebsprozesse innerhalb der BVG beeinträchtigt? Welche konkreten Arbeitsbereiche waren betroffen und wie wurde deren Handlungsfähigkeit sichergestellt?

Zu 9.: Die BVG teilt mit, dass der Ausfall des beauftragten Versand-Dienstleisters die Funktionalität zentraler Betriebsprozesse innerhalb der BVG nicht beeinträchtigt hat.

10. Wurde durch die BVG oder eine andere zuständige Stelle Strafanzeige erstattet? Falls ja, inwiefern wurden staatsanwaltliche Ermittlungen aufgenommen, und welcher Sachstand liegt hierzu vor?

Zu 10.: Die BVG teilt mit, dass sowohl der Dienstleister als auch die BVG Anzeige gegen Unbekannt gestellt haben.

11. Liegen der BVG oder den Ermittlungsbehörden bereits Erkenntnisse über die mutmaßlichen Täter oder deren Herkunft vor? Inwieweit wird ein gezielter Eingriff aus dem Ausland für möglich oder wahrscheinlich gehalten?

Zu 11.: Aufgrund des laufenden Ermittlungsverfahrens können von der BVG hier noch keine belastbaren Aussagen gemacht werden.

12. Welche technischen, organisatorischen oder vertraglichen Maßnahmen wurden seitens der BVG bzw. des betroffenen Dienstleisters ergriffen, um vergleichbare Sicherheitsvorfälle künftig zu verhindern und die Resilienz der Systeme nachhaltig zu erhöhen?

Zu 12.: Die BVG teilt mit, dass die Zusammenarbeit mit dem Dienstleister umgehend eingestellt wurde. Die Ursachen-Analyse – inklusive Ableitungen – befindet sich in Bearbeitung und wird intern intensiv vorangetrieben. Die Analyse ist aufgrund der Komplexität des Vorgangs und den noch laufenden Ermittlungen noch nicht abgeschlossen.

13. Inwiefern sieht die BVG das Risiko vergleichbarer Cyberangriffe auf kritische Systeme, insbesondere im Bereich des Fahrbetriebs? Welche präventiven Vorkehrungen und Notfallpläne bestehen, um im Ernstfall den Betrieb zu schützen und aufrechtzuerhalten?

Zu 13.: Die BVG teilt mit, dass sie die zunehmenden Cyberbedrohungen sehr ernst nimmt, insbesondere im Hinblick auf kritische Infrastrukturen wie den Fahrbetrieb. Als Betreiberin wesentlicher Teile der urbanen Mobilität in Berlin ist sich die BVG ihrer besonderen Verantwortung für die Sicherheit und Stabilität ihrer Systeme bewusst. Zum Schutz vor Cyberangriffen setzt die BVG nach eigenen Angaben auf ein mehrstufiges Sicherheitskonzept, das sowohl technische Sicherheitsvorkehrungen als auch organisatorische Maßnahmen umfasst. Die Systeme werden laufend überwacht, geprüft und weiterentwickelt. Die IT-Sicherheit wird durch ein zentrales Managementsystem gesteuert und regelmäßig auf neue Bedrohungslagen angepasst. Auch Mitarbeitende werden kontinuierlich sensibilisiert und geschult. Für den Fall eines sicherheitsrelevanten Vorfalls verfügt die BVG über abgestimmte Notfallpläne und Krisenreaktionsmechanismen. Diese dienen der schnellen Reaktion, der Schadensbegrenzung und der möglichst raschen Wiederherstellung des sicheren Betriebs. Die Pläne werden regelmäßig überprüft und mit relevanten Stellen abgestimmt.

Die BVG äußert, dass der aktuelle Vorfall keinerlei Auswirkungen auf kritische Systeme hatte. Der Fahrbetrieb war zu keinem Zeitpunkt beeinträchtigt. Unabhängig davon wurden die bestehenden Schutzmaßnahmen einer erneuten Überprüfung unterzogen und gezielt weiterentwickelt. Die BVG verfolgt einen ganzheitlichen Sicherheitsansatz, der sowohl Prävention als auch Reaktionsfähigkeit sicherstellt, um einen verlässlichen und sicheren Betrieb dauerhaft zu gewährleisten.

Berlin, den 03. Juni 2025

In Vertretung

Dr. Severin F i s c h e r

.....

Senatsverwaltung für Wirtschaft,
Energie und Betriebe