Abgeordnetenhaus BERLIN

Drucksache 19 / 22 581
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Christopher Förster (CDU)

vom 15. Mai 2025 (Eingang beim Abgeordnetenhaus am 16. Mai 2025)

zum Thema:

Hackerangriff auf die BVG

und **Antwort** vom 27. Mai 2025 (Eingang beim Abgeordnetenhaus am 2. Juni 2025)

Senatsverwaltung für Wirtschaft,
Energie und Betriebe

Herrn Abgeordneten Christopher Förster (CDU)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/22581
vom 15. Mai 2025
über Hackerangriff auf die BVG

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

Vorbemerkung der Verwaltung:
Die Schriftliche Anfrage betrifft zum Teil 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) um Stellungnahme gebeten, die von dort in eigener Verantwortung erstellt und dem Senat übermittelt wurde. Sie wird 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. Bei dem Dienstleister handelt es sich um ein Unternehmen, das die BVG beim professionellen Massenversand von Vertriebsschreiben unterstützt.
Die BVG hat die Berliner Datenschutzbehörde sowie die betroffenen Kundinnen und Kunden unverzüglich, nachdem gesicherte Kenntnis über Art und Umfang der Betroffenheit vorlagen, über den Vorfall informiert. Zur Aufklärung des Vorfalls sowie zur Klärung weiterer Schritte steht die BVG mit dem externen Dienstleister im Austausch. Sowohl der Dienstleister als auch die BVG haben Anzeige gegen Unbekannt gestellt.
Der Schutz personenbezogener Daten hat für die BVG höchste Priorität. Bei der Auswahl von Dienstleistern wird stets auf zertifizierte IT-Sicherheitsstandards geachtet. Wie es trotz der hohen Standards, nach denen die BVG ihre Dienstleister auswählt, zu diesem Vorfall kommen konnte, wird aktuell mit Hochdruck analysiert und aufgeklärt. Dieser Prozess ist noch nicht abgeschlossen. Die BVG hat die Geschäftstätigkeit mit dem Dienstleister vorsorglich

bis zum Abschluss einer umfassenden Prüfung der technischen Systeme und Datenflüsse einstweilen eingestellt.

1. Art und Umfang der kompromittierten Daten

a) Welche konkreten Kategorien von Kundendaten wurden nach aktuellem Kenntnisstand entwendet (z. B. Name, Postanschrift, E Mail-Adresse, Kunden- und Vertragsnummern)?

Zu 1. a: Die BVG teilt mit, dass folgende Daten nach aktuellem Kenntnisstand von dem Datenschutzvorfall betroffen sind:

- Name
- Postanschrift
- E-Mail-Adresse, sofern angegeben
- Kundennummer
- Vertragsnummer Berlin-Abo

1. b) Wurden auch besonders schützenswerte Daten (z. B. Ausweisdaten, Zahlungs- oder Kontodaten) erfasst?

Zu 1. b: Kontodaten und Passwörter sind nach Auskunft der BVG nicht betroffen. Bei den betroffenen Daten handele es sich um keine sensiblen Daten nach Art. 9 DSGVO (Datenschutz-Grundverordnung). Aktuell liegen der BVG keine Hinweise auf einen Missbrauch dieser Daten vor.

2. Anzahl der betroffenen Kunden

a) Wie viele Kundendatensätze sind insgesamt kompromittiert worden?

Zu 2. a: Die BVG teilt mit, dass durch den IT-Angriff auf den externen Dienstleister eine Datei mit 182.295 Kundendatensätzen, die die unter 1a) gelisteten Daten enthalten hat, betroffen ist.

2. b) Handelt es sich dabei um endgültig bestätigte oder geschätzte Werte?

Zu 2. b: Es handelt sich um endgültig bestätigte Werte.

3. Zeitlicher Ablauf des Vorfalls

a) Wann erfolgte der Angriff und wann wurde er durch den Dienstleister bzw. die BVG entdeckt?

Zu 3. a: Nach den der BVG vorliegenden Informationen des Dienstleisters erfolgte der IT-Angriff gegen den externen Dienstleister am 7. April 2025. Der Dienstleister hat am 8. April 2025 davon Kenntnis erlangt. Der Dienstleister meldete diesen Vorfall als einen nicht näher definierten allgemeinen Angriff auf seine IT Mitte April an die BVG. Gesicherte Kenntnis über Art und Umfang der BVG-Betroffenheit hatte die BVG am 30. April 2025.

3. b) Wie lange dauerte es vom Angriffsbeginn bis zur Unterbrechung des unbefugten Zugriffs?

Zu 3. b: Die BVG teilt hierzu mit, dass laut der Informationen des betroffenen Dienstleisters der Angriff rund 30 Minuten dauerte.

4. Informationspflicht und Kommunikationswege

a) Auf welchem Weg und in welchem zeitlichen Rahmen wurden die betroffenen Kunden sowie die Berliner Datenschutzbehörde informiert?

Zu 4. a: Die BVG hat nach eigener Auskunft alle Kundinnen und Kunden, deren Daten betroffen sind, per Brief über den Vorfall informiert. Nachdem die BVG am 30. April 2025 gesicherte Kenntnis über Art und Umfang der BVG-Betroffenheit hatte, seien unverzüglich die notwendigen Schritte zur Information der Berliner Datenschutzbehörde erfolgt. Diese wurde rund drei Stunden nach gesicherter Erkenntnis am 30. April 2025 informiert. Auch wurde von einer sofort eingesetzten Task Force die Erstellung eines Informationsschreibens veranlasst, dass alle betroffenen Kundinnen und Kunden informiert werden. Der Informationsbrief stand final und mit allen notwendigen Informationen am 5. Mai 2025 zur Verfügung und wurde ab dem 9. Mai 2025 an die Kundinnen und Kunden verschickt. Dazu war es notwendig, kurzfristig einen neuen Dienstleister zu verpflichten, der den Regularien der BVG entspricht und in der Lage war, kurzfristig und zuverlässig 180.000 Briefe zu versenden.
Weiterhin teilt die BVG mit, dass parallel zum Versand des Schreibens Kontaktmöglichkeiten für Rückfragen und Anliegen der Kundinnen und Kunden eingerichtet wurden sowie mit den Vorbereitungen für einen Fragen- und Antworten-Katalog auf der Seite der BVG gestartet wurde, der kontinuierlich die häufigsten Fragen der Kundinnen und Kunden beantwortet und Informationen aktualisiert. Auch die BVG-Mitarbeitenden der Hotline und in den Servicecentern wurden informiert, um Rückfragen der Kundinnen und Kunden zu beantworten.

5. Ermittlungs- und Aufklärungsmaßnahmen

a) Welche wesentlichen Schwachstellen und Angriffsvektoren wurden bislang identifiziert?

Zu 5. a: Die BVG teilt mit, dass sie sich im Austausch mit dem Dienstleister befindet und den Vorfall genau analysiert. Ziel sei es, eine transparente Aufarbeitung des Vorfalls zu erhalten, um damit auch für die Zukunft Ableitungen zu treffen. Dieser Prozess ist noch nicht abgeschlossen.
Nach dem aktuellen Kenntnisstand der BVG wurde der Angriff über eine Schwachstelle im Zeiterfassungstool des externen Dienstleisters eingeleitet. Weitere forensische Analysen und Auswertungen sind Teil der Aufarbeitung und der Ermittlungsprozesse.
Von diesem Angriff sind keine eigenen BVG-Systeme betroffen. Der Angriff erfolgte, nach Kenntnis der BVG, ausschließlich auf die IT-Infrastruktur des externen Dienstleisters.

6. Haftung und Vertragsprüfung

a) Welche vertraglichen Vereinbarungen zur Datensicherheit und Haftungsregelungen bestehen zwischen der BVG und dem betroffenen Dienstleister?
b) Gab es bereits rechtliche Schritte oder Schadenersatzforderungen gegenüber dem Dienstleister?

Zu 6. a und b: Die Fragen werden wegen ihres Sachzusammenhangs gemeinsam beantwortet. Die BVG teilt mit, dass die Zusammenarbeit mit dem nach ISO27001 zertifizierten Dienstleister auf einem schriftlichen Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO basiert, in dem die Anforderungen an den Schutz personenbezogener Daten, technische und organisatorische Maßnahmen (TOM) sowie die Meldepflichten bei Sicherheitsvorfällen verbindlich geregelt seien.
Darüber hinaus enthalte der zugrunde liegende Hauptvertrag verbindliche vertragliche Vereinbarungen zur Verfügbarkeit, Integrität und Vertraulichkeit der Datenverarbeitung sowie spezifische Haftungsregelungen für Datenschutzverstöße und Pflichtverletzungen. Diese Regelungen sehen vor, dass der Dienstleister für Schäden haftet, die auf eine Verletzung seiner vertraglichen oder gesetzlichen Pflichten zurückzuführen sind.
Die BVG prüfe derzeit im Rahmen der laufenden Aufarbeitung, ob und in welchem Umfang vertragliche oder gesetzliche Ansprüche geltend zu machen sind. Eine abschließende Bewertung etwaiger Ansprüche erfolgt erst nach Vorliegen aller relevanten Ergebnisse der technischen und rechtlichen Analyse.

7. Schutz- und Unterstützungsmaßnahmen für Betroffene

a) Welche konkreten Maßnahmen werden den betroffenen Kunden angeboten?

Zu 7. a: Direkt nach Bekanntwerden des Vorfalls wurde nach Informationen der BVG eine interdisziplinäre Task Force in der BVG eingerichtet, die den Vorfall eng begleitet und insbesondere auch Anfragen von BVG-Kundinnen und Kunden kategorisiert und schnellstmöglich beantwortet. Für die Rückfragen der betroffenen Kundinnen und Kunden sei ein Kontaktpostfach eingerichtet worden. Alle eingehenden Kundenanfragen seien umgehend beantwortet worden. Auch in den Kundenzentren erhalten betroffene Kundinnen und Kunden Hilfestellung.

8. Technische Sicherheitsverbesserungen

a) Welche technischen Maßnahmen (z. B. Verschlüsselung, Multi-Faktor-Authentifizierung, Zugriffsprotokollierung, Intrusion Detection Systems) waren zum Zeitpunkt des Angriffs implementiert?
b) Welche kurzfristigen und langfristigen technischen Maßnahmen plant die BVG zur Erhöhung der IT-Sicherheit, insbesondere im Umgang mit externen Partnern?

Zu 8. a und b: Die Fragen werden wegen ihres Sachzusammenhangs gemeinsam beantwortet. Die BVG teilt mit, dass sie sich im Austausch mit dem Dienstleister befindet und den Vorfall genau analysiert. Ziel ist es, eine transparente Aufarbeitung des Vorfalls zu

erhalten, um damit auch für die Zukunft Ableitungen zu treffen. Dieser Prozess ist noch nicht abgeschlossen.
Parallel und kurzfristig hat die BVG begonnen, bestehende Prozesse zur Zusammenarbeit mit externen Dienstleistern zu überprüfen und risikoorientiert nachzuschärfen. Dazu zählen insbesondere:

- eine Neubewertung aller Auftragsverarbeiter hinsichtlich Sicherheitsniveau und Auditierbarkeit,
- die Verpflichtung zu zeitnahen Schwachstellenmeldungen und Patchzyklen, also regelmäßigen Software-Updates, um eventuelle Sicherheitslücken zu schließen,
- die Einführung eines standardisierten Kontroll- und Eskalationsmechanismus bei Vorfällen.

Ziel sei ein ganzheitlicher Sicherheitsansatz, der nicht nur die BVG selbst, sondern auch ihre digital vernetzten Partner in die Pflicht nimmt.

9.Transparenz gegenüber der Öffentlichkeit

a) Wie viele Kundinnen und Kunden wurden bisher schriftlich und inhaltlich umfassend über den Vorfall informiert?
b) Welche Kommunikationswege (z. B. Brief, E Mail, BVG-Website, Kundenportal) wurden bzw. werden genutzt?
c) In welchem Zeitraum erhielten die Betroffenen ihre Mitteilung, und wie wird sichergestellt, dass alle tatsächlich betroffenen Personen erreicht werden?

Zu 9. a bis c: Die Fragen werden wegen ihres Sachzusammenhangs gemeinsam beantwortet. Die BVG teilt mit, dass alle rund 180.000 Kundinnen und Kunden, die betroffen sind, per Brief über den Vorfall informiert wurden. Betroffen können generell nur diejenigen Personen sein, die im Januar 2025 im Zusammenhang mit dem Tarifprodukt „Berlin Abo“ von der BVG kontaktiert oder informiert wurden. Bisher hat die BVG rund 500 Rückmeldungen zum Informationsbrief erhalten. Der weit überwiegende Teil der Rückmeldungen waren Fragen der Kundinnen und Kunden, die schnellstmöglich beantwortet wurden. Darüber hinaus aktualisiert die BVG kontinuierlich eine Informationswebseite auf www.bvg.de mit den häufigsten Nachfragen. Kundinnen und Kunden haben auch die Möglichkeit, über die BVG-Hotline oder analog in den Kundenzentren der BVG Antworten auf ihre Fragen zu erhalten.

10. Lehren und landesweite Maßnahmen

a) Welche Lehren und Konsequenzen zieht der Senat aus diesem Vorfall für alle landeseigenen Unternehmen und Behörden?

Zu 10. a: Der Senat unterstützt das Anliegen der BVG, den IT-Angriff auf das von der BVG beauftragte Unternehmen transparent aufzuarbeiten, um damit auch für die Zukunft Ableitungen zu treffen.
Da weder dieser Prozess noch das anhängige Verfahren bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit abgeschlossen ist, können zum jetzigen Zeitpunkt noch

keine abschließende Bewertung des IT-Angriffs vorgenommen und mögliche Konsequenzen aus diesem Vorfall seitens des Senats gezogen werden.

Berlin, den 27. Mai 2025

In Vertretung

Dr. Severin F i s c h e r
.....
Senatsverwaltung für Wirtschaft,
Energie und Betriebe