Abgeordnetenhaus BERLIN

Drucksache 19 / 20 941
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Niklas Schrader (LINKE)

vom 21. November 2024 (Eingang beim Abgeordnetenhaus am 22. November 2024)

zum Thema:

Wie sicher sind sensible Informationen bei der Berliner Polizei?

und **Antwort** vom 12. Dezember 2024 (Eingang beim Abgeordnetenhaus am 16. Dez. 2024)

Senatsverwaltung für Inneres und Sport

Herrn Abgeordneten Niklas Schrader (LINKE)

über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/20941
vom 21. November 2024
über Wie sicher sind sensible Informationen bei der Berliner Polizei

---

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

1. Medienberichten (https://www.tagesspiegel.de/berlin/sicherheitspanne-bei-der-polizei-berliner-erhalt-e-mails-aus-dem-anti-terror-zentrum-12650306.html) zufolge soll ein Berliner Polizeibeamter und Teilnehmer des Polizeiarbeitskreises der CDU einen E-Mailverkehr mit sensiblen Informationen zu Einschätzungen bezüglich der Terrororganisation Hamas aus dem “Gemeinsamen Terrorismus- und Extremismusabwehrzentrum” (GTAZ) unbefugt an einen unbeteiligten Bürger versendet haben.
    a. Welcher Geschehensablauf hat nach Kenntnis des Senats dazu geführt, dass sensible Lagebewertungen an einen unbefugten Empfänger gesendet wurden?
    b. Welcher Geheimhaltungsstufe unterlag der fehlgeleitete Inhalt?
    c. In welchem Ausmaß enthielt der fehlgeleitete Inhalt personenbezogene Daten?
    d. Inwiefern wurden alle möglichen Sicherheitsrisiken, die aus dem Vorfall resultieren, umfassend analysiert?
    e. Inwieweit wurde der Vorfall aufgearbeitet und welche Maßnahmen wurden seitdem eingeleitet, um solche Fehler zu vermeiden (spezielle Anweisungen, Schulungen für Mitarbeiter*innen)?
    f. Sind dem Senat weitere Personen bekannt, die den oben genannten E-Mail-Verlauf unbefugt erhalten haben? Wenn ja, wie viele?
    g. Wie wurde der oben genannte Empfänger der E-Mails nach Bekanntwerden des Verstoßes kontaktiert und welche Anweisungen hat er erhalten?

Zu 1. a.:
Nach derzeitigen Erkenntnissen der Polizei Berlin leitete eine Dienstkraft der Polizeidirektion (Dir) 4 (Süd) am 28. Oktober 2024 eine dienstliche E-Mail an verschiedene Adressaten – darunter auch an einen unberechtigten Empfänger – weiter.

Zu 1. b.:
Aufgrund der noch nicht abgeschlossenen Ermittlungen kann hierzu keine Aussage getroffen werden.

Zu 1. c.:
Der fehlgeleitete E-Mail-Verlauf enthielt personenbezogene Daten von 19 Dienstkräften (jeweils Vorname, Nachname, personalisierte dienstliche E-Mailadressen sowie zum Teil dienstliche Erreichbarkeiten, Verwendungsdienststellen und/oder Stellenzeichen). Darüber hinaus war für die Dienstkräfte, die diese E-Mail ebenso erhalten haben, Name und E-Mail-Adresse der Person, die Adressat der Fehlzustellung war, zu sehen. Im Inhalt der Mail waren weiterhin Hinweise zu Betreibern von Telegram-Kanälen und Inhalte dieser Kanäle enthalten. Hierbei handelt es sich um öffentlich zugängliche Informationen.

Zu 1. d.:
Durch die Dir 4 wurde die für die Informationssicherheit verantwortliche Dienstkraft in die Prüfung im Sinne der Fragestellung einbezogen. Darüber hinaus erfolgte eine Mitteilung an das Justiziariat der Polizei Berlin.

Zu 1. e.:
Der Sachverhalt wird durch die Dir 4 dienst- und disziplinarrechtlich geprüft. Darüber hinaus ist eine Sensibilisierung sämtlicher Mitarbeitenden der Polizei Berlin hinsichtlich des Umgangs mit E-Mails beabsichtigt.

Zu 1. f.:
Es wurde bekannt, dass der unbefugte Empfänger den E-Mail-Verlauf an mindestens 20 andere E-Mail-Empfänger weitergeleitet haben soll. Darüber hinaus kann aufgrund laufender Ermittlungen derzeit keine Aussage getroffen werden.

Zu 1. g.:
Der Empfänger wurde im Rahmen von Vorermittlungen durch die zuständige Fachdienststelle der Abteilung 3 des Landeskriminalamtes (LKA) Berlin angeschrieben und um Übersendung der vollständigen, hier in Rede stehenden Mail gebeten.

2. Wurde der Vorfall der Berliner Beauftragten für Datenschutz und Informationsfreiheit gemeldet und inwieweit wird er von dieser untersucht?

Zu 2.:
Bislang ist eine Meldung gemäß § 51 des Berliner Datenschutzgesetzes an die Berliner Beauftragte für Datenschutz und Informationsfreiheit zu diesem Sachverhalt nicht erfolgt, da die Prüfung durch das Justiziariat der Polizei Berlin ergab, dass nach bisherigen Erkenntnissen keine Gefahr für die Rechtsgüter natürlicher Personen besteht.

3. Welche Verschlüsselungs- oder Authentifizierungsmechanismen verwendet die Polizei für die E-Mail-Kommunikation mit anderen Behörden sowie bei der Kommunikation mit Bürger*innen?

Zu 3.:
Mit ausgewählten Behörden, darunter der Senatsverwaltung für Inneres und Sport, besteht eine Leitungsverschlüsselung zwischen den beteiligten E-Mail-Servern. Die Verwendung ist nur innerhalb des Landesnetzes möglich.

Als weitere Möglichkeit steht eine generelle Leitungsverschlüsselung im Corporate Network Polizei zur Verfügung. Über diese wird unter anderem die gesamte E-Mail-Kommunikation zwischen den Polizeien der Länder und des Bundes geführt.

Eine Verschlüsselung des E-Mail-Verkehrs zur Bevölkerung wird standardmäßig nicht verwendet.

Als eine vom BSI zugelassenen Standardlösung zur Verschlüsselung von E-Mail-Kommunikation bis zur Geheimhaltungsstufe VS-NfD ist z. B. die Software GnuPG im Land Berlin und auch bei der Polizei Berlin im Einsatz. Diese wird im Bedarfsfall für Verschlüsselungen genutzt.

4. Welche der am unter 1. genannten E-Mailverlauf beteiligten Behörden hat nach Kenntnis des Senats für diesen Informationsaustausch aus welchen jeweiligen Gründen keine
    a. E-Mail-Verschlüsselung und
    b. keine kryptografische Signatur verwendet?

Zu 4.:
Die betreffende Dienstkraft hat den Mailverlauf unverschlüsselt weitergeleitet. Insofern haben Verschlüsselungsmechanismen aus den vorgelagerten Mailverläufen hier keine Relevanz.

5. Welche Hinweise oder Vorfälle von welchem Datum und welchem Sachverhalt sind dem Senat aus den vergangenen 10 Jahren bekannt, bei denen Mitarbeiter*innen von Sicherheitsbehörden unbefugt Informationen per E-Mail preisgaben?

Zu 5.:
Vor dem Hintergrund der Einführung eines förmlichen Verfahrens zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 Datenschutzgrundverordnung bzw. § 51 BlnDSG im Jahr 2019 kann die Polizei Berlin erst ab diesem Zeitpunkt zur Anzahl der gemeldeten Vorfälle valide Aussagen treffen. Darüber hinaus erfolgt keine statistische Erhebung von Daten im Sinne der Fragestellung in der Polizei Berlin.

Im genannten Zeitraum seit 2019 wurden bei der Polizei Berlin Vorfälle im unteren einstelligen Bereich erfasst.

Am Amtsgericht Tiergarten sind für die vergangenen zehn Jahren keine Fälle unbefugter Informationsweitergabe per E-Mail bekannt. Im Übrigen ist eine statistische Auswertung aller Ermittlungsverfahren in Bezug auf unbefugte Informationsweitergaben per E-Mail schon deshalb nicht möglich, weil im Zuständigkeitsbereich der Senatsverwaltung für Justiz und Verbraucherschutz keine statistischen Anknüpfungsmerkmale erfasst werden.

6. In welchem Umfang und wie genau wurden vor dem Hintergrund der internationalen Vernetzung der Akteure der Hamas welche Behörden des Bundes, anderer Bundesländer oder anderer Staaten über den mutmaßlichen Informationsabfluss informiert?

7. Welche Auswirkungen hat der mutmaßliche Informationsabfluss auf die Zusammenarbeit im GTAZ; wann wurde der Vorfall dort in welcher Weise jeweils thematisiert?

Zu 6. und 7.:
Über den Informationsabfluss wurde nach Bekanntwerden im GTAZ berichtet. Nach bisheriger Bewertung des Vorfalls im GTAZ, erstmals am 4. November 2024, sind keine Auswirkungen auf die Zusammenarbeit erkennbar.

8. Gibt es Vorgaben des Senats zur regelmäßigen Überprüfung der IT-Sicherheit bei der Polizei und anderer sensibler Stellen?

Zu 8.:
Die Vorgaben bzw. Regelungen des Senats im Sinne der Fragestellung sind in der Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin (Informations-

sicherheitsleitlinie – InfoSic-LL) und den Grundsätzen zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung (IT-Sicherheitsgrundsätze) festgeschrieben.

Darüber hinaus erfolgt eine standardisierte bundesweite Zusammenarbeit der Polizeien des Bundes und der Länder. Bereits mit Beschluss vom 5. November 2002 hat der Arbeitskreis II (AK II) der Innenministerkonferenz auf seiner 190. Sitzung die Polizeien der Länder und des Bundes auf ein einheitliches hohes Sicherheitsniveau für ihre IT verpflichtet. Als Standard dafür wurde der IT-Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) festgelegt, welcher durch das jährlich aktualisierte IT-Grundschutz-Kompendium des BSI definiert ist.

Zur Überprüfung und Optimierung des erreichten Sicherheitsniveaus führen die Polizeien regelmäßig gegenseitige IS-Revisionen durch. Diese werden durch die Kommission IuK-Sicherheit (KomSi), Teil der Gremienstruktur unterhalb des AK II, verbundübergreifend geplant, koordiniert und ausgewertet.

Die KomSi ist auch verantwortlich für die Erarbeitung und Festsetzung von Mindeststandards in der IT-Sicherheit für die polizeilichen IT-Netze. So wurden 2022 überarbeitete Standards für die sichere E-Mail-Kommunikation verabschiedet.

9. Inwiefern plant der Senat, unabhängige Expert*innen für eine Untersuchung der IT-Systeme und der Sicherheit der E-Mail-Kommunikation einzusetzen?

Zu 9.:
Der Senat plant keine Aktivitäten, die über die unter Frage 8 genannten Vorgaben und Regelungen hinausgehen.

10. Inwiefern existiert ein regelmäßiger Austausch zwischen Polizei, Senat und externen IT-Experten zur Verbesserung der Datensicherheit?

Zu 10.:
Ein Austausch findet in regelmäßigen Abständen im Informationssicherheitsmanagement-Team (InfSiMa-Team) statt. Das InfSiMa-Team berät den Landesbeauftragten oder die Landesbeauftragte für Informationssicherheit zu strategischen oder behördenübergreifenden Aspekten der Informationssicherheit. Es besteht aus

- dem oder der Landesbeauftragten für Informationssicherheit (Vorsitz)
- den behördlichen Informationssicherheitsbeauftragten

- dem oder der Informationssicherheitsbeauftragten des IT-Dienstleistungszentrums Berlin.

Darüber hinaus können weitere Teilnehmende hinzugezogen werden. Den Informationssicherheitsbeauftragten der Verwaltung des Abgeordnetenhauses, des Rechnungshofs von Berlin und der BlnBDI steht die Teilnahme frei.

Darüber hinaus wird auf die unter Antwort zur Frage 8 aufgeführte standardisierte bundesweite Zusammenarbeit verwiesen.

11. Wie wird sichergestellt, dass sensible Informationen nur autorisierten Personen zugänglich gemacht werden?

Zu 11.:
Mit einer jährlichen Bekanntgabe gegen Unterschriftsleistung wird allen Dienstkräften der Polizei Berlin die Geschäftsanweisung zur Nutzung von Informations- und Kommunikationstechnik in der Polizei Berlin zur Kenntnis gegeben. Hierin ist u. a. geregelt, dass bei der Kommunikation zu dienstlichen Zwecken unter Nutzung der zur Verfügung gestellten Technik dienstliche Inhalte nur dem dafür bestimmten Adressatenkreis zur Kenntnis gelangen dürfen. Zudem ist gemäß der o. g. Geschäftsanweisung das Verschlüsseln von E-Mails stets dann geboten, wenn personenbezogene Daten übermittelt werden sollen und/oder eine Einstufung des Inhalts als „Verschlusssache (VS) – Nur für den Dienstgebrauch“ vorliegt und die Empfängeranschrift der E-Mail außerhalb der Polizeien des Bundes und der Länder liegt oder keine individuelle Leitungsverschlüsselung eingerichtet ist.

12. Welche Standards gelten für den Umgang mit Informationen, die innerhalb der Teilnehmerbehörden des GTAZ ausgetauscht werden?

Zu 12.:
Die Zusammenarbeit im GTAZ erfolgt fortwährend auf der Grundlage der Übermittlungsvorschriften der einschlägigen Bundes- und Landesgesetze sowie nach Maßgabe der jeweiligen Verschlusssachenanweisungen.

13. Welche Konsequenzen zieht der Senat aus dieser Sicherheitspanne, um solche Vorfälle zukünftig zu verhindern?

Zu 13.:
Innerhalb des betroffenen Dienstbereichs erfolgte eine Auswertung des Sachverhalts unter Hinzuziehung der für die Informationssicherheit verantwortlichen Dienstkraft. Der Sachverhalt wird durch die Polizei dienst- und disziplinarrechtlich geprüft. Darüber hinaus ist auch weiterhin eine kontinuierliche Sensibilisierung der Mitarbeitenden hinsichtlich des Umgangs mit E-Mails beabsichtigt.

14. Welche disziplinar- oder strafrechtlichen Verfahren und Maßnahmen wurden gegen den Beamten des Polizeiabschnitts ergriffen, durch dessen E-Mail-Kommunikation polizeiinterne Informationen mutmaßlich an Unbefugte abflossen?

Zu 14.:
Die dienst- und disziplinarrechtliche Prüfung des Sachverhaltes erfolgt durch die Polizei Berlin. Aus Gründen des Datenschutzes wird zu Personaleinzelangelegenheiten keine Auskunft erteilt.

15. Welche Dienstpflichtverletzungen durch Polizeidienstkräfte im CDU-Polizeiarbeitskreis sind dem Senat in den vergangenen 10 Jahren zur Kenntnis gelangt und welche Maßnahmen wurden daraufhin jeweils ergriffen? (Bitte aufschlüsseln nach Datum und Sachverhalt!)

Zu 15.:
Hier liegen keine Erkenntnisse im Sinne der Fragestellungen vor.

Berlin, den 12. Dezember 2024

In Vertretung

Christian Hochgrebe
Senatsverwaltung für Inneres und Sport