Abgeordnetenhaus BERLIN

Drucksache 17 / 13 301
Schriftliche Anfrage

17. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Thomas Birk (GRÜNE)

vom 26. Februar 2014 (Eingang beim Abgeordnetenhaus am 27. Februar 2014) und **Antwort**

E-Mail-Datenklau in Berlin

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

1. Wie viele E-Mail-Identitäten in welchen Berliner Behörden und öffentlichen Einrichtungen wurden beim im Januar 2014 bekannt gewordenen Massendiebstal von Zugangsdaten gestohlen?

Zu 1.: Von dem im Januar 2014 bekannt gewordenen Diebstahl von Zugangsdaten waren gemäß den der Senatsverwaltung für Inneres und Sport vorliegenden Informationen in der Berliner Verwaltung sieben Behörden mit insgesamt neun E-Mail-Adressen betroffen.

2. Welche Folgen hatte der Zugriff auf diese E-Mail-Adressen für die Datensicherheit auch bezüglich der Daten von Bürgerinnen und Bürgern, für die MitarbeiterInnen und die Sicherheit der IT-Systeme der betroffenen Behörde und der Verwaltung insgesamt?

Zu 2.: Nach den derzeit vorliegenden Erkenntnissen hatte der missbräuchliche Zugriff auf die oben angeführten Zugangsdaten keine negativen Folgen für die Datensicherheit der Daten von Bürgerinnen und Bürgern, für die Mitarbeiterinnen und Mitarbeiter und die Sicherheit der Informationstechnik-Systeme (IT-Systeme) der betroffenen Behörden und der Berliner Verwaltung insgesamt.

3. Trifft eine Pressemeldung zu, dass mehrere E-Mail-Adressen zusammengeschaltet wurden, um missbräuchlich Massenmails zu versenden?

Zu 3.: Dem Senat liegen dazu keine offiziellen Erkenntnisse vor.

4. Welche Sicherheitsvorkehrungen wurden in der Folge angeordnet?

Zu 4.: Von den Behörden wurden unterschiedliche Maßnahmen veranlasst, die auf den entsprechenden Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) basieren. Dazu zählen u. a.:

- Wechsel der Passwörter
- Gezieltes Überprüfen der IT-Systeme auf mögliche Schadsoftware
- Sensibilisierung der Beschäftigten zum sicheren Umgang mit Passwörtern.

5. Welche Grundsätze für die Vergabe und Anwendung von Passwörtern gelten für die Verwaltung und wie verbindlich sind diese?

6. Gibt es regelmäßige Intervalle innerhalb derer die Passwörter geändert werden müssen?

Zu 5. und 6.: Für die Vergabe und Anwendung von Passwörtern gelten in der Berliner Verwaltung die diesbezüglichen Regelungen des IT-Grundschutzkatalogs des BSI. Dazu zählen auch die Vorgaben bzgl. der Intervalle, in denen Passwörter gewechselt werden sollen.

7. Welches Controlling gibt es zu diesen Grundsätzen?

Zu 7.: Die dezentrale Umsetzung der einzelnen technisch-organisatorischen Sicherheitsmaßnahmen wie z. B. zur Anwendung und Gestaltung von Passwörtern obliegt gemäß der dezentralen Fach- und Ressourcenverantwortung den jeweiligen Behörden. Dazu zählt ebenso das gezielte Controlling zu den jeweiligen spezifischen Sicherheitsmaßnahmen.

Das übergreifende Controlling im Sinne einer ganzheitlichen Sicht auf Informationssicherheit erfolgt im Rahmen des jährlich von der Senatsverwaltung für Inneres und Sport erstellten Berichtes zur Informationssicherheit.

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

8. Wer ist grundsätzlich für die Erfassung und Koordinierung IT-sicherheitsrelevanter Angriffe auf das Land Berlin zuständig?

Zu 8.: Für die Behandlung von IT-Sicherheitsvorfällen mit behördenübergreifenden Auswirkungen gibt es ein definiertes Vorgehen mit festgelegten Abläufen, Kommunikationswegen und Verantwortlichkeiten. Die koordinierende Rolle obliegt dabei der Senatsverwaltung für Inneres und Sport in enger Abstimmung mit dem IT-Dienstleistungszentrum Berlin (ITDZ). Im Rahmen dieser koordinierenden Rolle hat die Senatsverwaltung für Inneres und Sport auch im vorliegenden Fall der missbräuchlichen Nutzung von Zugangsdaten die Behörden über vorliegende Erkenntnisse informiert. Die Umsetzung dezentral notwendiger Maßnahmen, mit denen auf den Sicherheitsvorfall reagiert und Schäden vermieden werden können, obliegt den jeweiligen Behörden (vgl. Antwort zu Frage 7).

Der bereits erwähnte Bericht zur Informationssicherheit enthält auch Angaben zu den IT-Sicherheitsvorfällen mit behördenübergreifenden Auswirkungen im jeweiligen Berichtsjahr.

Berlin, den 08. März 2014

Frank Henkel
Senator für Inneres und Sport

(Eingang beim Abgeordnetenhaus am 13. Mrz. 2014)