Deutscher Bundestag **Drucksache 16/10710**

16. Wahlperiode 27. 10. 2008

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Silke Stokar von Neuforn, Volker Beck (Köln), Monika Lazar, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 16/10513 –

Datenpannen bei Bundesbehörden

Vorbemerkung der Fragesteller

Auf Speichermedien, die in Bundesbehörden benutzt werden, befinden sich Daten, die für die innere und äußere Sicherheit relevant sind. Gerade die von den Bundesbehörden angelegten Datenbanken enthalten besonders schützenswerte personenbezogene Daten, die nicht für die Öffentlichkeit bestimmt, bzw. vertraulich oder geheim sind.

Bei privaten Unternehmen, aber auch bei der Zusammenarbeit von Behörden mit solchen Unternehmen ist es in der Vergangenheit wiederholt zu Datenpannen gekommen, so beispielsweise bei kommunalen Meldedaten. Mehr als drei Monate lang konnten die Meldedaten von etwa 500 000 Einwohnern – darunter Adressen, Passbilder und Religionszugehörigkeit – über die Internetseite „www.meldebehoerde.de“ eingesehen werden. Die Panne betraf bundesweit mehrere Städte (Quelle: Report München, „Schlampig und gefährlich – Der sorglose Umgang mit Daten bei Einwohnermeldeämtern“, Sendung vom 23. Juni 2008).

Ungeachtet dieser Vorfälle ist gerade das Bundesministerium des Innern bestrebt, weitere Datenbanken zu errichten und – entgegen der Rechtsprechung des Bundesverfassungsgerichtes (BVerfG) – immer mehr Daten auch auf Vorrat zu speichern. Es wird gearbeitet an einem bundesweiten Melderegister (vgl. den Aktionsplan unter www.deutschland-online.de, gesehen am 11. September 2008) und einer zentralen Abhöreinrichtung (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 16/10050).

Der Bundesminister des Innern, Dr. Wolfgang Schäuble, hat auf die Frage, ob die staatlich erhobenen und gespeicherten Daten sicher sind, geantwortet: „Sie sind sicherer als die Daten, die im privaten, nicht-öffentlichen Bereich umlaufen. Sie sind auch sicherer als in anderen europäischen Ländern“ (Quelle: Onlineinterview vom 25. August 2008, http://www.bundesregierung.de, gesehen am 11. September 2008).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 23. Oktober 2008 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Tatsächlich hat die Bundesregierung bereits eingeräumt, dass allein von 2005 bis 2007 in Bundesministerien und anderen Behörden 189 Tischcomputer und 326 Laptops verschwunden sind, davon 46 im Ausland. Außerdem gingen 271 Handys und Taschencomputer sowie 38 Speichersticks, CDs und DVDs mit Daten verloren oder wurden gestohlen. Die Daten waren zumindest teilweise nicht einmal verschlüsselt (vgl. die schriftlichen Fragen des Bundestagsabgeordneten Carl-Ludwig Thiele vom 6. März 2008 (Bundestagsdrucksache 16/8664, Nr. 24 und 25) und die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 16/8673). Die Ermittlungen der Staatsanwaltschaft wurden mittlerweile ohne Ergebnis eingestellt.

1. Aus welchen Datenbanken der Bundesbehörden sind nach Kenntnis der Bundesregierung seit April 2008 persönliche Daten an unbefugte Dritte gelangt, bzw. sind sie gestohlen worden oder sonst abhanden gekommen?

2. Auf welchem Speichermedium sind die Daten jeweils abhanden gekommen (CD, DVD, USB-Sticks, etc.)?

3. Welche von den jeweiligen Behörden gespeicherten Daten befanden sich auf den Speichermedien (Adressdaten, Bankverbindungsdaten)?

4. Sind darunter besonders schützenswerte Daten im Sinne des Bundesdatenschutzgesetzes (vgl. § 3 Abs. 9 des Bundesdatenschutzgesetzes – BDSG) gewesen?

6. Wurden diesbezüglich in allen Fällen Ermittlungsverfahren aufgenommen, und gegebenenfalls mit welchem Ergebnis?

Soweit in der Kürze der Zeit feststellbar, sind aus Datenbanken von Bundesbehörden seit April 2008 nur in einem Fall eines entwendeten Notebooks möglicherweise persönliche Daten an Unbefugte gelangt. Der Verdacht, dass sich auf dem gestohlenen Notebook eine alte Kopie einer Datenbank mit Umsatzsteuerbetrugsfällen befand, ließ sich im Nachhinein nicht mehr sicher entkräften. Es könnte sich auch um eine Datenbank mit Test- bzw. Schulungsdaten gehandelt haben. Kenntnisse über Ermittlungsergebnisse aufgrund der zum Fall erstatteten Strafanzeige liegen bislang nicht vor.

5. Welche Vorkehrungen hat die Bundesregierung seit dem Bekanntwerden der letzten Datenpanne getroffen, um künftige Ereignisse dieser Art zu vermeiden?

7. Welche Vorkehrungen wird die Bundesregierung künftig treffen, um weitere Datenpannen dieser Art zu vermeiden?

8. Wie beurteilt die Bundesregierung diesbezüglich die Eignungsbeurteilungen und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) – die bisher keine Bindewirkung haben – für den weiten Bereich zwar sensitiver, formal jedoch nicht als Verschlusssache eingestufter Daten?

Vorkehrungen zur Vermeidung von Datenpannen sind ein wesentlicher Teil der Daueraufgabe, IT-Sicherheit zu gewährleisten. Das Kabinett hat in Umsetzung des Nationalen Plans zum Schutz der Informationsinfrastrukturen in Deutschland (NPSI) am 5. September 2007 einen „Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (UP Bund) verabschiedet. Dieser bildet die verbindliche IT-Sicherheitsleitlinie für die Bundesverwaltung.

Die laufende Umsetzung der darin festgelegten Maßnahmen verbessert auch den Schutz vor Datenpannen.

Nach dieser verbindlichen IT-Sicherheitsleitlinie sind die BSI- Standards 100-1 (Managementsysteme für Informationssicherheit), 100-2 (IT-Grundschutz-Vorgehensweise) und 100-3 (Risikoanalyse auf der Basis von IT-Grundschutz) in der Bundesverwaltung anzuwenden. Darin wird sehr ausführlich darauf eingegangen, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist. Im Zusammenspiel mit den IT-Grundschutz-Katalogen werden konkrete Hinweise gegeben, wie eine Umsetzung (auch auf technischer Ebene) aussehen kann. Die sich daraus ergebenden Maßnahmen beinhalten selbstverständlich auch angemessene Vorkehrungen zum Schutz sensitiver, formal jedoch nichts als Verschlusssache eingestufter Daten sowie zur weiteren Minimierung von Datenverlusten. Angesichts entsprechender Vorfälle in Großbritannien sind die Ressorts Anfang Februar diesen Jahres noch einmal gebeten worden, die Anwendung der im Umsetzungsplan festgelegten Sicherheitsstandards zu überprüfen.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333