12703/J XXV. GP

Eingelangt am 03.04.2017

Anfrage

der Abgeordneten Dr. Jessi Lintl
und weiterer Abgeordneter
an den Bundesminister für Inneres
betreffend Datensicherheitskonzepte und – maßnahmen des Bundes

Laufend wird in den Medien von Hackerattacken berichtet, wie beispielsweise von dem Vorfall, bei welchem türkische Hacker die Zeitungswebsite oe24.at durch eine DDos Attacke lahmgelegt haben, wie vom Innenministerium bestätigt wurde.[1] Ebenso wurde das Außenministerium Opfer türkischer Hacker, wie aus einem Artikel der Tageszeitung Presse hervorgeht.[2]

Dem Einsatz externer Dienstleister in Ministerien und staatlichen Institutionen ist daher vor allem im IT-Bereich erhöhte Aufmerksamkeit zu schenken und entsprechende Sicherheitsvorkehrungen zu treffen.

Der Datenschutzrat hat in einem Schreiben an den Herrn Bundeskanzler, alle Bundesministerinnen und Bundesminister sowie an die Frau Staatssekretärin und den Herrn Staatssekretär vom 28. März 2014 die einzelnen Bundesministerinnen und Bundesminister ersucht, ihre Datensicherheitskonzepte und die ihrer nachgeordneten Dienststellen, ihrer ausgegliederten Unternehmen, ihrer Dienstleister sowie ihrer Werksauftragsnehmer insbesondere hinsichtlich der Einhaltung der Datensicherheitsmaßnahmen nach § 14 DSG 2000 zu überprüfen. Anlassfall dazu war die unzulässige Veröffentlichung von 400.000 BIFIE-Schultestdaten sowie 37.000 Lehrer- und Schulleiterdaten (e-mail Adressen) auf einem externen Server.

Der Datenschutzrat verweist in diesem Schreiben ausdrücklich auch auf die im DSG 2000 geregelten Voraussetzungen zur Heranziehung eines Dienstleisters.

Darüber hinaus empfiehlt der Datenschutzrat, dass bundesweit eine zentrale Anlaufstelle für Meldungen über Datensicherheitsvorfälle betraut werden sollte, um

[1] *Quelle: http://derstandard.at/2000054358500/Tuerkische-Hacker-legten-Zeitungswebseite-oe24at-lahm*
[2] *Quelle: http://diepresse.com/home/innenpolitik/5179179/Tuerkische-HackerAttacke-auf-Aussenministerium*

ein geordnetes Krisenmanagement bei derartigen Verletzungen der Datensicherheit zu gewährleisten.

In diesem Sinne sollte im Lichte des § 14 Abs. 1 und 2 DSG 2000 geprüft werden, ob

• die **Aufgabenverteilung** bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festgelegt ist,

• die Verwendung von Daten an das Vorliegen **gültiger Aufträge** der anordnungsbefugten Organisationseinheiten und Mitarbeiter gebunden sind,

• jeder Mitarbeiter über seine nach dem DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften **bestehenden Pflichten belehrt wurde**,

• die **Zutrittsberechtigung zu den Räumlichkeiten** des Auftraggebers oder Dienstleisters geregelt ist,

• die **Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger** vor der Einsicht und Verwendung durch Unbefugte geregelt ist,

• die **Berechtigung zum Betrieb der Datenverarbeitungsgeräte** festgelegt und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen **gegen die unbefugte Inbetriebnahme abgesichert ist,**

• **Protokoll** geführt wird, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,

• eine **Dokumentation** über die getroffenen Maßnahmen geführt wird, um die Kontrolle und Beweissicherung zu erleichtern.

In diesem Zusammenhang richten die unterfertigten Abgeordneten an den Bundesminister für Inneres nachstehende

ANFRAGE

1) Haben Sie, bzw. wurde von Ihrem Ressort im Lichte des § 14 Abs. 1 und 2 DSG 2000 geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festgelegt ist?

2) Wenn nein, warum nicht?

3) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

4) Haben Sie, bzw. wurde von Ihrem Ressort im Lichte des § 14 Abs. 1 und 2 DSG 2000 geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten gebunden sind?

5) Wenn nein, warum nicht?

6) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

7) Wurden Daten auch ohne das Vorliegen gültiger Aufträge der anordungsbefugten Organisationseinheiten verwendet?

8) Wenn ja, wie oft? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., nach Datum der unbefugten Verwendung)

9) Ist durch diese unbefugten Datenverwendungen ein Schaden entstanden?

10) Wenn ja, wie hoch war die Schadenssumme? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und nach dem jeweiligen Vorfall unter Anführung des Datums des Erkennen des Schadens)

11) Haben Sie, bzw. wurde von Ihrem Ressort im Lichte des § 14 Abs. 1 und 2 DSG 2000 geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern jeder Mitarbeiter über seine nach dem DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten belehrt wurde?

12) Wenn nein, warum nicht?

13) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

14) Hat es Fälle in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern gegeben, in denen Mitarbeiter über ihre nach dem DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten nicht belehrt wurden?

15) Wenn ja, wie viele Fälle? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und Datum der Prüfung)

16) Haben Sie, bzw. wurde von Ihrem Ressort im Lichte des § 14 Abs. 1 und 2 DSG 2000 geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters geregelt ist?

17) Wenn nein, warum nicht?

18) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

19) Hat es Fälle in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern gegeben, bei welchen es Verletzungen der Regelungen der Zutrittsberechtigungen gegeben hat?

20) Wenn ja, wie viele Fälle? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und Datum der Prüfung)

21) Ist durch diese Verletzungen der Regelungen der Zutrittsberechtigungen ein Schaden entstanden?

22) Wenn ja, wie hoch war die Schadenssumme? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und nach dem jeweiligen Vorfall unter Anführung des Datums des Erkennen des Schadens)

23) Haben Sie, bzw. wurde von Ihrem Ressort im Lichte des § 14 Abs. 1 und 2 DSG 2000 geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte geregelt ist?

24) Wenn nein, warum nicht?

25) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

26) Hat es Fälle in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern gegeben, bei welchen es Verletzungen der Regelungen der Zugriffsberechtigungen auf Daten und Programme und der

Regelungen zum Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte gegeben hat?

27) Wenn ja, wie viele Fälle? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und Datum der Prüfung)

28) Ist durch diese Verletzungen der Regelungen der Zugriffsberechtigungen und der Regelungen zum Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte ein Schaden entstanden?

29) Wenn ja, wie hoch war die Schadenssumme? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und nach dem jeweiligen Vorfall unter Anführung des Datums des Erkennen des Schadens)

30) Haben Sie, bzw. wurde von Ihrem Ressort im Lichte des § 14 Abs. 1 und 2 DSG 2000 geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festgelegt und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abgesichert ist?

31) Wenn nein, warum nicht?

32) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

33) Hat es Fälle in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern gegeben, bei welchen es Verletzungen der Regelungen gab, welche die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festlegen?

34) Wenn ja, wie viele Fälle? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und Datum der Prüfung)

35) Ist durch diese Verletzungen der Regelungen über die Berechtigung zum Betrieb der Datenverarbeitungsgeräte ein Schaden entstanden?

36) Wenn ja, wie hoch war die Schadenssumme? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und nach dem jeweiligen Vorfall unter Anführung des Datums des Erkennen des Schadens)

37) Haben Sie, bzw. wurde von Ihrem Ressort im Lichte des § 14 Abs. 1 und 2 DSG 2000 geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern Protokoll geführt wird, damit tatsächlich durchgeführte Verwendungsvorgänge, wie

insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit in notwendigen Ausmaß nachvollzogen werden können?

38) Wenn nein, warum nicht?

39) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

40) Hat es Fälle in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern gegeben, bei welchen es Verletzungen der Regelungen über die Protokollführung gem. Frage 37 gab?

41) Wenn ja, wie viele Fälle? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und Datum der Prüfung)

42) Haben Sie, bzw. wurde von Ihrem Ressort im Lichte des § 14 Abs. 1 und 2 DSG 2000 geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern eine Dokumentation über die getroffenen Maßnahmen geführt wird, um die Kontrolle und Beweissicherung zu erleichtern?

43) Wenn nein, warum nicht?

44) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

45) Hat es Fälle in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern gegeben, bei welchen es Verletzungen der Regelungen über die Dokumentation gem. Frage 42 gab?

46) Wenn ja, wie viele Fälle? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und Datum der Prüfung)

47) Haben Sie, bzw. wurde von Ihrem Ressort geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen und in Ihren ausgegliederten Unternehmen die Regelungen des § 10 DSG 2000, wonach Auftraggeber bei ihren Datenanwendungen Dienstleister in Anspruch nehmen dürfen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten und der Auftraggeber mit dem Dienstleister die hiefür notwendigen Vereinbarungen zu treffen hat und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen hat?

48) Wenn nein, warum nicht?

49) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

50) Hat es Fälle in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern gegeben, bei welchen es Verletzungen der Regelungen des § 10 DSG 2000 gab?

51) Wenn ja, wie viele Fälle? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und Datum der Prüfung)

52) Ist durch diese Verletzungen der Regelungen des § 10 DSG 2000 ein Schaden entstanden?

53) Wenn ja, wie hoch war die Schadenssumme? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und nach dem jeweiligen Vorfall unter Anführung des Datums des Erkennen des Schadens)

54) Haben Sie, bzw. wurde von Ihrem Ressort geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen und in Ihren ausgegliederten Unternehmen die Regelungen des § 11 Abs 1 DSG 2000 eingehalten wurden, wonach unabhängig von allfälligen vertraglichen Vereinbarungen, Dienstleister bei der Verwendung von Daten für den Auftraggeber jedenfalls die im leg. cit Pflichten haben, insbesondere auch die Verpflichtung, die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden, alle gemäß § 14 DSG 2000 erforderlichen Datensicherheitsmaßnahmen zu treffen und weitere Dienstleister („Subdienstleister“) nur mit Billigung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann?

55) Wenn nein, warum nicht?

56) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

57) Hat es Fälle in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern gegeben, bei welchen es Verletzungen der Regelungen des § 11 DSG 2000 gab?

58) Wenn ja, wie viele Fälle? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und Datum der Prüfung)

59) Ist durch diese Verletzungen der Regelungen des § 11 DSG 2000 ein Schaden entstanden?

60) Wenn ja, wie hoch war die Schadenssumme? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und nach dem jeweiligen Vorfall unter Anführung des Datums des Erkennen des Schadens)

61) Haben Sie, bzw. wurde von Ihrem Ressort geprüft, ob in Ihrem Ressort, in Ihren nachgeordneten Dienststellen und in Ihren ausgegliederten Unternehmen die Regelungen des § 24 Abs 2a DSG 2000 eingehalten wurden, wonach der Auftraggeber, wenn ihm bekannt wird, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, darüber unverzüglich die Betroffenen in geeigneter Form zu informieren hat („Data breach notification)?

62) Wenn nein, warum nicht?

63) Wenn ja, welche Resultate hat die Prüfung bzw. haben die Prüfungen ergeben? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., Zeitraum der Prüfung und Prüfungsergebnis)

64) Hat es Fälle in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern gegeben, bei welchen es Verletzungen der Regelungen des § 24 Abs. 2a DSG 2000 gab?

65) Wenn ja, wie viele Fälle? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und Datum der Prüfung)

66) Ist durch diese Verletzungen der Regelungen des § 11 DSG 2000 ein Schaden entstanden?

67) Wenn ja, wie hoch war die Schadenssumme? (Bitte aufgliedern nach geprüfter Einheit, wie beispielsweise Ressort, nachgeordnete Dienststelle, ausgegliedertes Unternehmen etc., und nach dem jeweiligen Vorfall unter Anführung des Datums des Erkennen des Schadens)

68) Wurde nach der Empfehlung des Datenschutzrates im Jahr 2014 in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern eine Anlaufstelle für Meldungen über Datensicherheitsvorfälle eingerichtet?

69) Wie viele Datenschutzvorfälle hat es in Ihrem Ressort, in Ihren nachgeordneten Dienststellen, in Ihren ausgegliederten Unternehmen, bei Ihren herangezogenen Dienstleistern und bei Ihren Werksauftragnehmern in den Jahren 2014 bis 2016 gegeben?