1551/AB
vom 16.06.2020 zu 1544/J (XXVII. GP)

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.321.123

Wien, am 16. Juni 2020

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Dr. Stephanie Krisper, Kolleginnen und Kollegen haben am 16. April 2020 unter der Nr. **1544/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Rubicon Datenleck“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur Frage 1:

- *Besteht nach wie vor ein Vertragsverhältnis zwischen der Rubicon IT GmbH und dem Innenministerium?*
  a. *Wenn ja, wurden im Zusammenhang mit der medialen Berichterstattung ab September 2019 Vertragsanpassungen von Seiten des Ministeriums mit der Rubicon IT GmbH durchgeführt?*
  b. *Wie hoch war das Entgelt für die Jahre 2011 bis 2019, welches die Rubicon IT GmbH vom BMI erhalten hat (bitte um genaue Auflistung nach Jahren)?*
  c. *Wie hoch waren die Ausgaben für Entwicklung und Implementierung von PAD (bitte um genaue Auflistung nach Jahren)?*
  d. *Wie hoch waren die Ausgaben für Entwicklung und Implementierung von IKDA (bitte um genaue Auflistung nach Jahren)?*
  e. *Wie hoch waren die Ausgaben für Entwicklung und Implementierung von VStV BMI (bitte um genaue Auflistung nach Jahren)?*

f. *Wie hoch waren die Ausgaben für Entwicklung und Implementierung von Sirene (bitte um genaue Auflistung nach Jahren)?*

Es besteht nach wie vor ein Vertragsverhältnis zwischen der Rubicon IT GmbH und dem Bundesministerium für Inneres. Vertragsanpassungen zwischen dem Bundesministerium für Inneres und der Firma Rubicon IT GmbH wurden nicht vorgenommen.

Jahr	Entgelt (inkl. USt)	Ausgaben für Entwicklung und Implementierung PAD und VStV* (inkl. USt)	Ausgaben für Entwicklung und Implementierung IKDA (inkl. USt)	Ausgaben für Entwicklung und Implementierung von Sirene (inkl. USt.)
2011	719.737,20		714.937,20	4.800,00
2012	1.916.568,00	1.720.320,00	0.00	0,00
2013	1.934.325,60	1.544.232,00	113.040,00	280.805,04
2014	4.471.487,52	3.459.060,00	17.280,00	12.408,00
2015	807.058,50	591.399,00	93.312,00	29.232,00
2016	10.915.107,14	7.342.301,64	6.168,00	73.485,00
2017	1.311.944,50	765.724,30	156.721,20	167.040,00
2018	4.325.340,54	2.615.558,12	0,00	175.030,51
2019	5.663.487,66	1.146.686,74	91.539,00	0,00
Summe	**32.065.056,66**	**19.185.281,80**	**1.192.997,40**	**742.800,55**

* In dieser Tabelle sind die Kosten für das VStV und das PAD angeführt. Eine Trennung der Kosten zwischen VStV und PAD ist nicht möglich, da das VStV ein Teil des PAD ist.

Zur Frage 2:

- *In einer Mail vom 1.3.2019 von „BMI II/BK-Projekt IKDA", das intern im Ministerium versendet wurde, wird von Abänderungswünschen von der Rubicon IT GmbH gesprochen. Ist dem Innenminister dieses Mail bekannt?*
  a. *In der Mail werden unter Punkt 5 Bedenken geäußert, dass lt. Mitteilung der Betriebsführung (IV/2) der Rubicon IT GmbH für PAD und SIRENE trotz Sicherheitsbedenken der Betriebsführung Zugang gewährt wurde. Welche Konsequenzen zog das Innenministerium wann aus den angemeldeten Sicherheitsbedenken durch Setzen welcher Maßnahmen?*

i. Wenn keine Maßnahmen getroffen wurden, warum nicht?

b. *Laut der Mail gab es im ersten Quartal 2019 die Forderung von Seiten der Rubicon GmbH nach einem „Remote-Zugang" zum Referenzsystem. Ist das richtig?*
   i. Wenn ja, warum wurde der Rubicon IT GmbH ein solcher Zugang gewährt?
   ii. Ist oder war es im Innenministerium üblich, dass externe Anbieter unkontrollierte Remotezugänge zu klassifizierten Informationen bekommen?
      1. Wenn ja, wann wurde dies welchem externen Anbieter zu welchen/r Bereich/Datenbank gewährt?
   iii. Welche Unternehmen haben oder hatten Remote-Zugriff zu klassifizierten Informationen?
   iv. Bei welchen Unternehmen und zu welchen Datenbanken wird oder wurde ein solcher Zugriff wann registriert (bitte um ausführliche Liste)?
   v. Wurde Unternehmen gegenüber auf eine Registrierung oben genannter Zugriffe verzichtet?
      1. Wenn ja, wann gegenüber welchen Unternehmen?
      2. Wenn ja, warum?

Das angesprochene E-Mail vom 1. März 2019 datiert aus der vorigen Gesetzgebungsperiode. Da ich zu diesem Zeitpunkt nicht Bundesminister für Inneres war und die diesbezügliche Frage persönlich den Wissenstand eines meiner Amtsvorgänger betrifft, kann ich dazu auch keine Stellungnahme abgeben.

Remote-Zugänge sind ausdrücklich in den Allgemeinen Vertragsbedingungen des Bundes als Standard für die Erbringung von Wartungsleistungen vorgesehen und eine vertragliche Bedingung, damit bestimmte Reaktionszeiten bei Wartungsleistungen eingefordert werden können. Jedoch werden Remote-Zugänge für Wartungszwecke im Bundesministerium für Inneres nur restriktiv vergeben.

Um die Sicherheit bei Remote-Zugängen auf allen Ebenen zu gewährleisten, werden die folgenden Maßnahmen seitens des Bundesministeriums für Inneres gesetzt:

- Remote-Zugänge werden strikt personenbezogen und nur für jene Systeme vergeben, welche die Person für ihre Aufgabenerfüllung benötigt.
- Remote-Zugänge werden nur nach erfolgter und anstandsloser Sicherheitsüberprüfung gemäß § 55 Sicherheitspolizeigesetz Personen gewährt.
- Alle für das Bundesministerium für Inneres tätigen Personen haben eine Verpflichtungserklärung zur Einhaltung des Datengeheimnisses gemäß § 6 Datenschutzgesetz zu unterzeichnen.

- Sämtliche Zugriffe über Remote-Zugänge werden mitprotokolliert und sind dementsprechend nachvollziehbar.

Als Reaktion auf die im gegenständlichen Fall geäußerten Sicherheitsbedenken wurden die für Wartungszwecke bestehenden Remote-Zugänge umgehend gesperrt.

Der Rubicon IT GmBH wurde ein Remote-Zugang zum Referenzsystem „BMI II/BK-Projekt IKDA“ nicht gewährt.

Kein Unternehmen hat einen Remote-Zugriff zu klassifizierten Informationen im Bundesministerium für Inneres. Bei den von der gegenständlichen Anfrage umfassten Systemen handelt es sich nicht um Systeme mit klassifizierten Informationen. Im Übrigen darf ich auf die Beantwortung der Fragen 23 bis 27 der Anfrage 4192/J XXVI. GP (4171/J XXVI. GP) des Abgeordneten Jenewein vom 25. September 2019 durch meinen Amtsvorgänger verweisen.

Zur Frage 3:

- *Laut Anfragebeantwortung (4171/AB) bestätigt das BMI, dass es für die Rubicon IT GmbH bis März 2019 Remotezugänge gegeben hat.: „Zutreffend ist, dass am 1. März 2019 für Wartungszwecke bestehende Remotezugänge für Mitarbeiter des Auftragsverarbeiters gesperrt wurden.“ (siehe Seite 8 der AB)*
  a. *Zu welchen Datenbanken gab es diese Remote-Zugänge?*
  b. *Seit wann gab es diese Remote-Zugänge (bitte um Aufzählung nach einzelnen Datenbanken)?*
  c. *Mit welchen (technischen) Berechtigungen waren die zuständigen Mitarbeiter, welche über diese Zugänge verfügten, ausgestattet (bitte um Aufzählung nach einzelnen Datenbanken)?*
  d. *Umfassten diese (technischen) Berechtigungen auch die Möglichkeit, Daten zu löschen oder zu verändern (bitte um Aufzählung nach einzelnen Datenbanken?*
  e. *Wurden die Zugriffe „zu Wartungsarbeiten“ der Rubicon IT GmbH protokolliert?*
     i. Wenn ja, sind dies Protokollierungen noch vorhanden (bitte um Auflistung)?

Die Mitarbeiter der Rubicon IT GmbH hatten bzw. haben im Rahmen eines Wartungsvertrages Remote-Zugriff. Diese Zugriffe erfolgten bzw. erfolgen zum Zweck der Wartung, Support und Betriebsunterstützung und umfassen bei den angeführten Systemen die Berechtigung zu suchen, lesen und schreiben. Zwei Remote-Zugriffe bei den Systemen PAD und VStV umfassten auch die Berechtigung zu löschen.

- PAD (Protokollieren-Daten Anzeigen), seit 2018;

- VStV: Automationsunterstützte Führung von Verwaltungsstrafverfahren, seit 2015;
- IKDA - Integrierte Kriminalpolizeiliche Datenanwendung, seit 2014;
- SIRENE Österreich (Supplementary Information Request at the National Entry); seit 2019.

Sämtliche Zugriffe auf Systeme des Bundesministeriums für Inneres werden nachvollziehbar mitprotokolliert. Diese Protokolldaten sind vorhanden. Ein Zugriff auf diese Protokolldaten ist aber nur unter engen rechtlichen Voraussetzungen möglich, weshalb eine Auflistung auch nicht möglich ist.

Zur Frage 4:

- *Gab es von Seiten ausländischer Behörden (vor allem von Ministerien aus Schengenstaaten) Kontaktaufnahmen mit dem BMI aufgrund der Berichterstattung im Zusammenhang mit dem Datenleck?*
  a. *Wenn ja, vonseiten welcher Behörden welcher Ministerien welcher Staaten und wann erfolgten diese Kontaktaufnahmen (bitte um ausführliche Auflistung)?*
  b. *Gab es Sicherheitsbedenken von ausländischen Behörden, was den Zugriff der Rubicon IT GmbH auf SIRENE (oder andere Datenbanken) betrifft?*
     i. Wenn ja, welche von welchen Behörden welcher Ministerien welcher Staaten und wann wurden diese Sicherheitsbedenken geäußert?
     ii. Wenn ja, wie hat das BMI auf diese Bedenken wann und durch welche Maßnahmen reagiert?

Nein.

Zur Frage 5:

- *Die Rubicon IT GmbH hat laut einstimmigen Medienberichten den Zuschlag vom BMI ohne Ausschreibung erhalten. Nach welchen Kriterien wurden und werden die in Frage kommenden Unternehmen vom BMI eingeladen?*
  a. *Welche externen Experten wurden dafür herangezogen (bitte um Auflistung)?*
     i. Zu welcher Schlussfolgerung kamen die einzelnen Experten?
  b. *Welchen anderen Unternehmen, neben Rubicon, wurden für diesen Auftrag vom BMI eingeladen?*

Auftragsvergaben richten sich nach dem Bundesvergabegesetz und den darin festgelegten Kriterien.

Zur Frage 6:

- *Der damalige Innenminister Dr. Peschorn hat eine ausführliche Untersuchung zum Datenleck angekündigt. Wurde diese Untersuchung begonnen?*
  a. *Wenn ja, wann wurde diese Untersuchung gestartet?*
  b. *Wenn ja, wer führte diese Untersuchung durch?*
  c. *Wenn ja, zu welchem Ergebnis ist diese Untersuchung wann gekommen?*

Die Untersuchung wurde unmittelbar nach Erscheinen des Zeitungsartikels vom 18. September 2019 eingeleitet und durch die zuständige IT-Abteilung gemeinsam mit den für die Anwendungen zuständigen Fachabteilungen unter Einbindung der Datenschutzbeauftragten des Bundesministeriums für Inneres durchgeführt. Zusätzlich war vom Bundesministerium für Inneres die Einbindung der Datenschutzbehörde geplant, diese hat jedoch eigenständig ein Prüfverfahren eingeleitet.

Die ersten Ergebnisse waren bereits im September 2019 verfügbar und haben bei den Zugriffen keine Auffälligkeiten gezeigt. Weitere Ergebnisse der Untersuchung wurden im Rahmen des Prüfverfahrens der Datenschutzbehörde im Oktober, November und Dezember 2019 an die Datenschutzbehörde übermittelt, wobei im Rahmen der Auswertungen und Analysen keine Auffälligkeiten seitens der Datenschutzbehörde festgestellt wurden.

Zur Frage 7:

- *In der Beantwortung der Anfrage 4192/J „Datenlecke Rubicon" spricht der damalige Innenminister in der Beantwortung der Fragen 23 bis 27 von einem „angeblichen Datenleck", obwohl im internen Mail von Viktor W. vom 01.03.2019 an hochrangige IT-Experten des BMI festgestellt wird, dass „sämtliche Zugriffe und Aktivitäten die direkt auf die Datenbank erfolgen, nicht protokolliert sind" und „dass keine Überwachung durch Betrieb IV/2/c möglich ist." Allgemein wird ein nicht kontrollierbarer und nicht protokollierter Zugang zu Daten als Datenleck bezeichnet.*
  a. *Woraus ergeben sich diese unterschiedlichen Einschätzungen des ehemaligen Innenministers und der hochrangigen IT-Experten des BMI?*
     i. *Welche Auffassung hatte welcher Experte (bitte um genaue Auflistung)?*
     ii. *Welcher Auffassung war das BMI und wie kam man zu dieser?*
        1. *Was ist nach der Ansicht des BMI ein Datenleck?*
     iii. *Warum entstanden diese Divergenzen und wie sahen diese aus?*

Es bestand keine unterschiedliche Einschätzung. Das angeführte E-Mail ist falsch zitiert. Aus Gründen der Amtsverschwiegenheit wird aber von einer Darlegung interner Diskussionsprozesse Abstand genommen.

Bei Zweifeln im Sicherheitsbereich werden im Bundesministerium für Inneres in jedem Fall unverzüglich die entsprechenden Maßnahmen zur Absicherung der Systeme gesetzt und umgehend Analysen durchgeführt. Die Untersuchungen im gegenständlichen Fall haben ergeben, dass es keine Auffälligkeiten gab und gibt.

Laut dem Datenschutz-Grundsatzerlass des BMI ist ein Datenleck bzw. eine „Verletzung des Schutzes personenbezogener Daten“ (iSd Art. 4 Z 12 DSGVO, § 36 Abs. 2 Z 11 DSG) eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Zur Frage 8:

- *Sind dem BMI alle Zugriffe seitens der Rubicon IT GmbH seit 2007 auf die Produktionsumgebungen PAD, IKDA, VStV BMI und SIRENE bekannt?*
  a. *Wenn ja, seit wann sind welche Zugriffe bekannt?*
  b. *Wenn ja, wie viele gab es?*
  c. *Wenn nein, wurden Maßnahmen getroffen, um an diese Informationen zu kommen?*
     i. Wenn ja, wann wurden dafür welche Maßnahmen gesetzt?
  d. *Gab es Anzeigen und Klagen seitens des BMI von der bzw gegen die Rubicon IT GmbH?*
     i. Wenn ja, mit welchem Inhalt?
     ii. Wenn nein, warum nicht?
  e. *Gegen wie viele Beamt_innen wurde wann ein Ermittlungsverfahren wegen der Veröffentlichung der Dokumente eingeleitet?*

Jeder der insgesamt 17 Zugriffe inklusive Datums wurde ab dem Zeitpunkt der Implementierung mitprotokolliert. Gegen die Rubicon IT GmbH gab es keine Anzeigen bzw. Klagen, da kein Grund hierfür bestand.

Da sich aus der Fragestellung nicht erhellt, welche Dokumente gemeint sind, ist eine seriöse Beantwortung nach allfällig eingeleiteten Ermittlungsverfahren nicht möglich.

Sollte sich jedoch die Frage nach den eingeleiteten Ermittlungsverfahren auf die Veröffentlichung der abgebildeten Dokumente die in den beiden in der Präambel erwähnten Artikel beinhaltet waren, beziehen, muss auf Grund eines laufenden Ermittlungsverfahrens von einer Beantwortung dieser Frage Abstand genommen werden.

Zu den Fragen 9 bis 12:

- *Wann wurde das Programm PAD im BMI implementiert?*
- *Wann wurde das Programm IKDA im BMI implementiert?*
- *Wann wurde das Programm VStV BMI im BMI implementiert?*
- *Wann wurde das Programm Sirene im BMI implementiert?*

PAD wurde am 15. Jänner 2018, IKDA am 29. September 2014, VStV am 3. März 2014 und Sirene am 24. Jänner 2009 implementiert.

Zur Frage 13:

- *Gab es Schulungen zur Verwendung von polizeilichen Datenbanken in Bezug auf Sicherheitsmaßnahmen und Datenschutz?*
  a. *Wenn ja, wie viele Schulungen gab es?*
  b. *Wenn ja, wann wurden diese abgehalten?*
  c. *Wenn ja, in welchen Intervallen werden solche Schulungen durchgeführt?*
  d. *Wenn nein, warum gab es keine Schulungen in Bezug auf Sicherheitsmaßnahmen und Datenschutz?*
  e. *Wenn nein, ist geplant, derartige Schulungen vorzunehmen?*
     i. *Wenn ja, wann?*

Alle Mitarbeiter der IKT-Abteilungen des Bundesministeriums für Inneres haben zweimal jährlich eine Awareness-Schulung hinsichtlich IKT-Sicherheit zu absolvieren. Die Schulungen wurden im Jahr 2019 im April und Mai (1. Themenblock) und von Ende Oktober bis Anfang Dezember (2. Themenblock) durchgeführt. Zusätzliche geplante Maßnahmen sind ein E-Learning-Modul und die Bereitstellung von Awareness-Beiträgen.

Für IKDA gab es keine speziell auf Sicherheitsmaßnahmen und Datenschutz ausgerichteten Schulungen. Das Thema wird in den Endanwenderschulungen zur Handhabung der Applikation unter Verweis auf die für IKDA erlassene Büroordnung mitbehandelt. Darin ist im Abschnitt 6 angeordnet: „Jede Bearbeitung hat unter Einhaltung der gesetzlichen Grundlage zu erfolgen“.

Karl Nehammer, MSc

	Datum/Zeit	2020-06-16T15:38:01+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1710479
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-06-16T15:43:52+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	