1315/AB
vom 25.05.2020 zu 1304/J (XXVII. GP)

Bundesministerium
Arbeit, Familie und Jugend

bmafj.gv.at

Mag. (FH) Christine Aschbacher
Bundesministerin

christine.aschbacher@bmafj.gv.at
+43 1 711 00-0
Untere Donaustraße 13-15, 1020 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.204.771

Wien, am 25.05.2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 25.03.2020 unter der **Nr. 1304/J** an mich eine schriftliche parlamentarische Anfrage betreffend **Rahmenvereinbarung Cybersecurity** gerichtet.

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

Zu den Fragen 1 und 2

- *Wurden seit Feststellung des Cyberangriffs auf das BMEIA von Seiten Ihres Ressorts sowie nachgelagerten Stellen oder Behörden spezielle Maßnahmen getroffen, um die eigenen IKT-Systeme besser abzusichern?*
  - *Wenn ja, welche? Bitte um Auflistung nach Maßnahmen und angefallenen Kosten.*
  - *Wenn nein, warum nicht?*
- *Sind bereits vor Feststellung des Cyberangriffs auf das BMEIA vonseiten Ihres Ressorts sowie nachgelagerten Stellen oder Behörden Maßnahmen getroffen worden, um die eigenen IKT-Systeme besser abzusichern?*
  - *Wenn ja, welche? Bitte um Auflistung nach Jahr, Maßnahmen und angefallenen Kosten.*
  - *Wenn nein, warum nicht?*

Im Zuge der Vorfallsbehandlung im BMEIA wurden durch den interministeriellen Einsatzstab sowohl laufende Risikoeinschätzungen, als auch Empfehlungen für konkrete Absicherungen der eigenen Netze erstellt und kommuniziert. Alle diese Maßnahmen wurden zeitnah durch die verantwortlichen Techniker in den Ministerien und im BKA umgesetzt. Weiters wurden die jeweiligen kritischen Systeme engmaschig überprüft und Maßnahmen ergriffen eine Kompromittierung weiterer Systeme (z.B. Personalverwaltung) hintanzuhalten.

Darüber hinaus erfolgen Maßnahmen zur IT-Sicherheit im Arbeitsmarktservice (AMS) und in der IEF Service GmbH nicht anlassbezogen aufgrund eines Angriffs auf andere Einrichtungen, sondern kontinuierlich. Dazu zählen neben der Sicherstellung der Systemvoraussetzungen etwa auch die Schulung der Mitarbeiter/innen in Zusammenhang mit Cybersicherheit aber auch Penetrationstests oder Sicherheitsaudits. Es bestand keine Notwendigkeit nach Feststellung des Cyberangriffs auf das BMEIA spezifische Maßnahmen zu setzen. Eine Evaluierung des Status Quo im Sozial- und Weiterbildungsfonds wies mit Blick auf IT-Risiken nach dem Cyberangriff keine Notwendigkeit aus, weitere Maßnahmen zusätzlich zu den bestehenden zu ergreifen.

Des Weiteren wird hier auf die Beantwortung der parlamentarischen Anfrage 1299/J durch das Bundeskanzleramt verwiesen.

Zu den Fragen 3 und 4

- *Welche Beschaffungen zur Verbesserung der Sicherheit der eigenen IKTSysteme wurden seit Feststellung des Cyberangriffs auf das BMEIA vonseiten Ihres Ressorts bzw. nachgelagerten Stellen oder Behörden getätigt?*
    - *Bestehen Rahmenvereinbarungen bezüglich dieser Beschaffungen?*
        - *Wenn ja, welche?*
        - *Zwischen welchen Parteien wurden diese Rahmenvereinbarungen geschlossen?*
        - *Welche Leistungen wurden in diesen Rahmenvereinbarungen vereinbart?*
        - *War es dem/den Vertragspartner/n Ihres Ressorts bzw. nachgelagerten Stellen oder Behörden möglich, alle vereinbarten Leistungen selbst zu erbringen?*
        - *Mussten Leistungen vom Auftragnehmer in Kooperation mit Dritten erbracht werden?*
            - *Wenn ja, mit welchen Kooperationspartnern?*

- *Welche Leistungen wurden von den Kooperationspartnern erbracht? Bitte um separate Aufschlüsselung nach Kooperationspartner.*

- *Welche Stundensätze wurden von den Unternehmen, die nach Bekanntwerden des Cyberangriffs auf das BMEIA Leistungen erbrachten, veranschlagt? Wie hoch waren die Gesamtkosten? Bitte um separate Aufschlüsselung der Stundensätze und Gesamtkosten pro Unternehmen.*

- *Gab es hier Ausschreibungen laut Bundesvergabegesetz?*
  - *Wenn ja, für welche Leistungen?*
  - *Wenn nein, warum nicht? Bitte um Übermittlung der vergaberechtlichen Bestimmungen.*

- *Welche Beschaffungen zur Verbesserung der Sicherheit der eigenen IKTSysteme wurden vor dem Cyberangriff auf das BMEIA von seiten Ihres Ressorts bzw. nachgelagerten Stellen oder Behörden getätigt?*
  - *Bestehen bzw. bestanden Rahmenvereinbarungen bezüglich dieser Beschaffungen?*
    - *Wenn ja, welche?*
    - *Zwischen welchen Parteien wurden diese Rahmenvereinbarungen geschlossen?*
    - *Welche Leistungen wurden in diesen Rahmenvereinbarungen vereinbart?*
    - *War es dem/den Vertragspartner/n Ihres Ressorts bzw. nachgelagerten Stellen oder Behörden möglich, alle vereinbarten Leistungen selbst zu erbringen?*
    - *Mussten Leistungen vom Auftragnehmer in Kooperation mit Dritten erbracht werden?*
      - *Wenn ja, mit welchen Kooperationspartnern?*
      - *Welche Leistungen wurden von den Kooperationspartnern erbracht? Bitte um separate Aufschlüsselung nach Kooperationspartner.*
    - *Welche Stundensätze wurden von diesen Unternehmen veranschlagt? Wie hoch waren die Gesamtkosten? Bitte um separate Aufschlüsselung der Stundensätze und Gesamtkosten pro Unternehmen.*
  - *Gab es hier Ausschreibungen laut Bundesvergabegesetz?*
    - *Wenn ja, für welche Leistungen?*
    - *Wenn nein, warum nicht? Bitte um Übermittlung der vergaberechtlichen Bestimmungen.*

Es wird in diesem Zusammenhang auf die Beantwortung der parlamentarischen Anfrage 1299/J durch das Bundeskanzleramt verwiesen.

Darüber hinaus hat das **AMS** seine IT an externe Dienstleister im Sinne eines Generalunternehmers ausgelagert. Das Sicherheitsmanagement ist ein integraler Bestandteil der Zusammenarbeit mit den beiden derzeitigen IT Dienstleistern (IBM Österreich & BRZ GmbH), die vertraglich zur Etablierung eines angemessenen Sicherheitsniveaus der AMS-IT Systeme verpflichtet sind. Die Implementierung von Maßnahmen erfolgt in Abstimmung mit dem AMS und wird regelmäßig hinsichtlich Zweckmäßigkeit und Effektivität überprüft. Rahmenvereinbarungen, die ausschließlich die Sicherung der IKT-Systeme beinhalten, bestehen nicht. Die Durchführung der Dienstleistungen durch die genannten Generalunternehmer erfolgte teilweise unter Zuhilfenahme externer Security Dienstleister.

Seit dem Cyberangriff auf das BMEIA wurden keine zusätzlichen Beschaffungen getätigt und daher auch keine zusätzlichen Rahmenvereinbarungen abgeschlossen. Bei nach dem Cyberangriff auf das BMEIA stattfindende Sicherheitsaudits handelte es sich um im Vorfeld geplante Tests, die in keinerlei ursächlichen Zusammenhang mit dem Angriff gegen das BMEIA stehen. Es sind keine zusätzlichen Kosten angefallen.

Der Vertrag mit der IBM Österreich wurde nach einer Ausschreibung laut Bundesvergabegesetz geschlossen. Der Vertrag mit der BRZ GmbH wurde auf Basis einer Schwesternvergabe gem. BVergG geschlossen.

Das IKT-System der **IEF Service GmbH** unterliegt besonders in Bezug auf die IT-Sicherheit einem laufenden Verbesserungs- und Optimierungsprozess. Vor Jahren schon wurde im Rahmen der Einführung des Qualitätsmanagementsystems ein Prozess zur Schließung eventueller Sicherheitslücken, zur Optimierung der bestehenden IT-Sicherheit sowie zur Sicherstellung einer stabilen Betriebskontinuität etabliert.

Es bestehen folgende Rahmenvereinbarungen im Sinne der Anfrage:

Vorweg ist darauf hinzuweisen, dass die Bekanntgabe des Firmennamens den verfolgten Zweck der Sicherheit gefährden könnten, daher sind diese im Folgenden anonymisiert dargestellt.

1. Firma A GmbH für die Lieferung von Hard- und Software sowie laufende Wartungsarbeiten. Der Stundensatz lag bei € 144,00 inkl. USt. Der Gesamtauftrag belief sich auf € 81.318,07 inkl. USt. Davon entfielen € 6.912,00 auf Dienstleistung.
2. Firma B GmbH für die Implementierung eine Policy inkl. Wartung und Systemaktualisierung. Der Stundensatz lag bei € 168,00 inkl. USt. Der Gesamtauftrag belief sich auf € 36.692,40 inkl. USt. Davon entfielen € 1.344,00 auf Dienstleistung.
3. Firma C GmbH: Wartung von zusätzlichen Cybersicherheitssystemen. Da keine Dienstleistungen vorgesehen sind, wurde kein Stundensatz verrechnet. Der Gesamtauftrag belief sich auf € 6.040,44 inkl. USt.

Den Vertragspartnern war es möglich, die Leistungen selbst zu erbringen. Leistungen der Auftragnehmer mussten nicht in Kooperation mit Dritten erbracht werden.

Die Rahmenverträge wurden nicht ausgeschrieben. Im einen Fall erfolgte ein Abruf aus der Rahmenvereinbarung der BBG. Bei den anderen Rahmenverträgen handelte es sich um Direktvergaben.

Im **Sozial- und Weiterbildungsfonds** unterteilen sich die gesetzten Maßnahmen zur Verbesserung der IKT-Systeme einerseits in Anschaffung und andererseits in den Zukauf von Beratungsleistungen und IT-Betreuung in Form von Einzelverträgen.

Es bestehen bzw. bestanden keine Rahmenverträge. Folgende Einzelverträge wurden abgeschlossen:

1. Firma D: Beratung und Umsetzung von EDV-technischen Lösungen, allgemeine Arbeiten zur Gewährleistung der IKT Sicherheit (Updates, Störungsbehebung, Systemzugänge). Der Stundensatz lag bei € 96 inkl. USt. Die Gesamtkosten belaufen sich auf € 5.251,83.
2. Firma E GmbH: laufendes Hosting von Datenbank, E-Mailsystem, Zertifikaten, der Cloud und der Webseite. Die Verrechnung erfolgt nicht per Stundensatz. Die Gesamtkosten belaufen sich auf € 19.944,30.
3. Firma F GmbH: laufende Beratung hinsichtlich Datenschutz, Risikoabschätzungen, Adaptierungen und technischer Umsetzung. Der Stundensatz liegt bei € 247,50 inkl. USt. Gesamtkosten belaufen sich auf € 12.650,88 inkl. USt.
4. Firma G: Sicherheitsrelevante Funktionalitäten, Updates und Tests für die eigene Fachapplikation sowie für Drittmodule. Die Gesamtkosten lagen bei € 38.698,25 inkl. USt. Der Stundensatz lag bei € 90 inkl. USt.

Ausschreibungen laut Bundesvergabegesetz erfolgten aufgrund der niedrigen Auftragssummen nicht.

Zu Frage 5

- *Welche internen Abteilungen sind für die IKT-Sicherheit Ihres Ministeriums zuständig?*
    - *Wie viele Mitarbeiter_innen hat/haben diese Abteilung/en?*
    - *Auf welcher Rechtsgrundlage basieren/basierten diese Arbeitsverhältnisse? Um Angabe der Zahl der Beschäftigten nach Art der Rechtsverhältnisse wird ersucht:*
        - *Beamtendienstverhältnis*
        - *Vertragsbedienstetenverhältnis*
            - *Befristet*
            - *unbefristet*
        - *Freie Dienstnehmer_innen*
        - *Werkvertrag*
        - *Arbeitskräfteüberlassung*
        - *Sonstige*
    - *Wie viele dieser Personen sind/waren mit spezifischen "Cybersecurity Tätigkeiten" im technischen Sinn befasst?*

Es darf in diesem Zusammenhang auf die Geschäftseinteilung verwiesen werden. Die Mitarbeiter und Mitarbeiterinnen der IKT-Sicherheit arbeiten in einem sensiblen Bereich und müssen vor kriminellen Aktivitäten und nachrichtendienstlicher Ausspähung geschützt werden. Daher muss von einer konkreten Nennung von Anzahl und Einstufung Abstand genommen werden.

Mag. (FH) Christine Aschbacher

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR ARBEIT, FAMILIE UND JUGEND @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Arbeit, Familie und Jugend
	Datum/Zeit	2020-05-25T18:26:08+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	743463191
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-05-26T07:59:59+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.	