

## **Anfrage**

**der Abgeordneten Dr. Stephanie Krisper, Kolleginnen und Kollegen  
an den Bundesminister für Inneres  
betreffend Rubicon Datenleck**

Am Mittwoch, den 18.9.2019 wurde auf der Homepage der Plattform "[fass-ohne-boden.at](https://www.fass-ohne-boden.at)" der Artikel „BMI-Datenleck: Programmierer konnten unbemerkt auf Polizeidaten zugreifen“ veröffentlicht (<https://www.fass-ohne-boden.at/bmi-datenleck-programmierer-konnten-unbemerkt-auf-polizeidaten-zugreifen/>). Dieser Artikel zitiert ein internes Schreiben aus dem BMI. Daraus lässt sich entnehmen, dass die RUBICON IT GmbH bzw. deren Mitarbeiter\_innen uneingeschränkten Zugriff auf sensible Daten des BMI und deren nachgeordnete Dienststellen hatte. Auf Basis des oben angeführten Artikels und der Beantwortung der Anfrage 4192/J ergeben sich einige Fragen.

Die unterfertigten Abgeordneten stellen daher folgende

### **Anfrage:**

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)?
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?
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)?
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?
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?
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?
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?
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?
9. Wann wurde das Programm PAD im BMI implementiert?
10. Wann wurde das Programm IKDA im BMI implementiert?
11. Wann wurde das Programm VStV BMI im BMI implementiert?
12. Wann wurde das Programm Sirene im BMI implementiert?
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?

The bottom of the page contains several handwritten signatures and scribbles. From left to right, there is a signature that appears to be 'Kuback', a large scribble, a signature that looks like 'Bayer', another signature, and a signature that looks like 'Künzel'. There are also some illegible scribbles and a signature that looks like 'H. S. ...'.

