4192/J
vom 25.09.2019 (XXVI.GP)

Anfrage

des Abgeordneten Jenewein
und weiterer Abgeordneter
an den Bundesminister für Inneres
betreffend Datenleck Rubicon

Am Mittwoch den 18.09.2019 veröffentlichte die Internet Recherche Plattform „fass-ohne-boden.at" auf ihrer Homepage (https://www.fass-ohne-boden-at/bmi-datenleck-programmierer-konnten-unbemerkt-auf-polizeidaten-zugreifen) einen Artikel mit der Überschrift: BMI-Datenleck: Programmierer konnten unbemerkt auf Polizeidaten zugreifen.

Demnach hatte die Firma RUBICON bzw. deren Mitarbeiter uneingeschränkten Zugriff auf sensibelste Daten des BMI und deren nachgeordnete Dienststellen.
Betroffen davon ist ua das Bundeskriminalamt mit dem Programm IKDA, aber auch sämtliche behördlichen Informationen aus dem Sicherheitsbereich in ganz Österreich. Im IKDA des Bundeskriminalamtes werden sämtliche Informationen gespeichert und der Schriftverkehr des Bundeskriminalamtes abgewickelt.
Das PAD und PAD-NG wird von allen Polizeidienststellen in ganz Österreich zur Erstattung von Anzeigen und Berichten verwendet.
Die Firma RUBICON erstellte für das BVT das Programm EDIS, welches dem Programm IKDA des Bundeskriminalamtes gleicht.
Im EDIS sind aktuell rund 250.000 klassifizierte Dokumente gespeichert.

In diesem Zusammenhang stellen die unterfertigten Abgeordneten an den Bundesminister für Inneres folgende

Anfrage

1. Was wird mit dem Programm EDIS im BVT bearbeitet/verarbeitet/gespeichert?
2. Welche Informationen werden nach dem InfoSiG-Informationssicherheitsgesetz klassifiziert?
3. Gilt dieses Gesetz auch für die LVTs-Landesämter für Verfassungsschutz und Terrorismusbekämpfung und andere nachgeordnete Sicherheitsbehörden?
    a. Wenn nein, warum nicht?
4. Welche Informationen werden nach der GehSO-Geheimschutzordnung klassifiziert?
5. Wie werden Informationen im BVT klassifiziert?
6. Nach welchen gesetzlichen Bestimmungen werden diese Informationen im BVT klassifiziert?
7. Wo werden die klassifizierten Dokumente im BVT aufbewahrt?
8. Warum werden die gesetzlichen Bestimmungen zur Klassifizierung nicht eingehalten?
9. Wie erfolgt die Bearbeitung der klassifizierten Dokumente?
    a. Vor der „BVT-Razzia" am 28.02.2018?
    b. Nach der „BVT-Razzia" am 28.02.2018?

10. Werden diese klassifizierten Dokumente auch elektronisch bearbeitet/verarbeitet?
11. Ist das EDIS System im BVT dafür zertifiziert?
    a. Wenn ja, seit wann?
    b. Wenn ja, von wem erfolgte die Zertifizierung?
    c. Wenn nein, warum nicht?
12. Ist das E-Mail System im BVT dafür zertifiziert?
    a. Wenn ja, seit wann?
    b. Wenn ja, von wem erfolgte die Zertifizierung?
    c. Wenn nein, warum nicht?
13. Warum werden die klassifizierten Dokumente im EDIS gespeichert, bearbeitet und verarbeitet?
14. Warum werden die klassifizierten Dokumente im E-Mail System gespeichert, verschickt, bearbeitet und verarbeitet?
15. Wurde die ISK-Informationssicherheitskommission davon wie vorgesehen informiert
    a. Wenn nein warum nicht?
16. Im EDIS-Handbuch befindet sich eine Dienstanweisung des BVT-Direktors, wonach Partnerdienst-Infos im EDIS zu speichern sind?
17. Wie viele Informationen von Partnerdiensten finden sich nach wie vor im EDIS?
18. Mit welchen Ländern gilt das InfoSiG, wenn Informationen gekennzeichnet sind
    a. Sind Informationen von diesen Ländern, die gekennzeichnet sind, im EDIS gespeichert?
    b. Werden oder wurden Informationen von diesen Ländern, die entsprechend gekennzeichnet sind, per Dienstanweisung intern via E-Mail versendet?
19. Liegt mit der Fa RUBICON ein entsprechender Vertrag und Vertragsabschluss vor?
    a. Wenn ja, wo befindet sich der Vertrag nun?
    b. Wenn nein, warum ist der Vertrag nicht vorhanden?
    c. Wenn nein, warum erfolgen trotz Fehlen des Vertrages weiterhin die Zahlungen an die Firma RUBICON?
    d. Entspricht es der Wahrheit, das für das Servicepaket der Firma RUBICON eine Jahrespauschale von 1 Million Euro zu bezahlen ist?
    e. Entspricht es der Wahrheit, dass für eine Rufbereitschaft der Firma RUBICON monatlich der Betrag von € 10.000 Euro zu bezahlen ist?
20. Wurde das Programm EDIS entsprechend den vertraglichen Vereinbarungen umgesetzt?
    a. Wenn nein, warum nicht?
21. Wurde die volle vereinbarte Summe für das Programm EDIS bezahlt?
    a. Wenn ja, wann und in welcher Höhe?
22. Entspricht es der Wahrheit, das der ehemalige Kabinettschef Michael KLOIBMÜLLER oder eine andere derzeit unbekannte Person die Weisung erteilt hat, das Programm EDIS, obwohl es noch nicht fertig ist, abzunehmen und in den Echtbetrieb überzugehen.?
    a. Wenn ja, wer hat diese Weisung erteilt?
    b. Wenn ja, wann ist diese Weisung ergangen?
    c. Wenn nein, ist das EDIS gemäß den für den Vertragsabschluss vereinbarten Parameter im Pflichtenheft fertiggestellt?

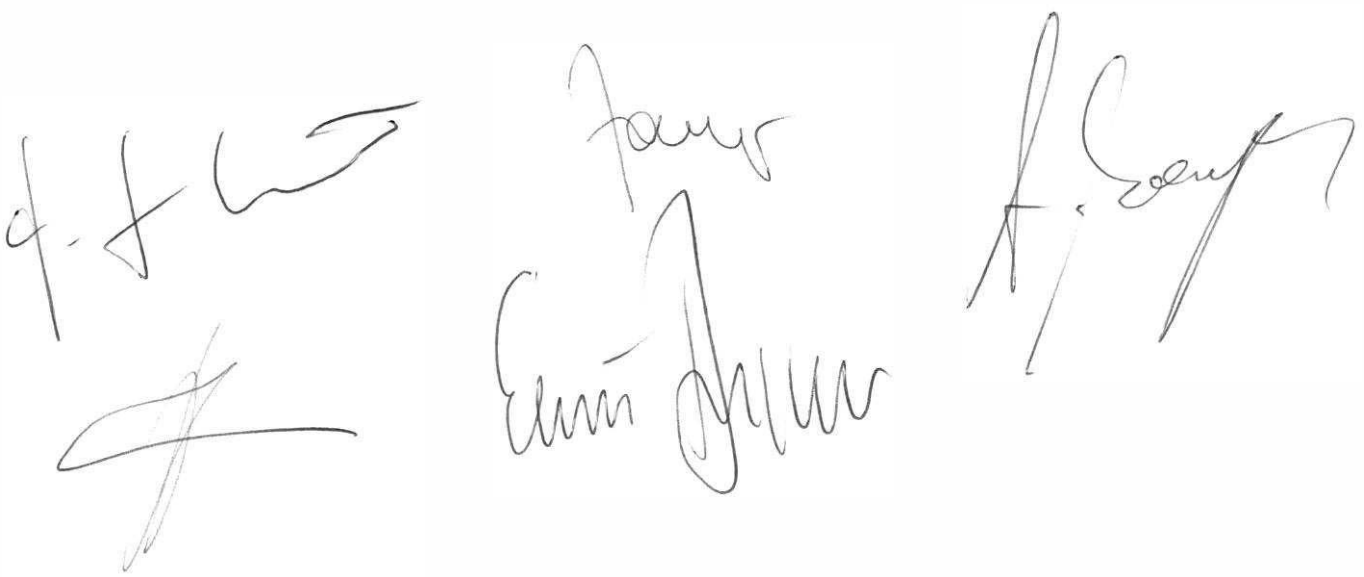
   d. Wenn nein, warum nicht?
23. Berührt das nunmehr medial bekannte Daten-Leak auch das BVT?
24. Hatte die Fa RUBICON einen Fernzugriff auf das EDIS Programm im BVT?
25. Ist es Mitarbeitern der Fa RUBICON theoretisch möglich gewesen, innerhalb des BVT auf Echtdaten im EDIS zuzugreifen?
   a. Wenn ja, ist dies den Partnerdiensten bekannt?
   b. Wenn nein, kann dies zu 100% ausgeschlossen werden?
26. Ist es Mitarbeitern der Fa RUBICON theoretisch möglich gewesen, von außerhalb des BVT auf Echtdaten im EDIS zuzugreifen?
   a. Wenn ja, ist dies den Partnerdiensten bekannt?
   b. Wenn nein, kann dies zu 100% ausgeschlossen werden?
27. Entspricht es der Wahrheit, das Mitarbeiter der Fa RUBICON für das BVT Datenlöschungen im EDIS durchgeführt haben?
28. War das Programm EDIS bevor Herbert KICKL Innenminister wurde, zertifiziert?
   a. Wenn nein, warum nicht?
29. Ist das E-Mail System von der ISK-Informationssicherheitskommission im Bundeskanzleramt zertifiziert?
   a. Wenn ja, seit wann?
   b. Wenn nein, warum nicht?
30. Wurde der Umstand, dass das Programm und die gesamte EDV-Ausstattung (PC, Laptop, Server, E-Mail Server, Mobiltelefone, Smartphones) des BVT von der ISK-Informationssicherheitskommission im Bundeskanzleramt nicht zertifiziert ist, den Partnerdiensten verschwiegen?
31. Ist es gesetzlich verboten, klassifizierte Informationen ab der Stufe Vertraulich im EDIS zu speichern?
32. Ist dieser Umstand, dass klassifizierte Informationen im EDIS gespeichert werden, obwohl das System nicht dafür zertifiziert ist, dem jeweiligen Informationssicherheitsbeauftragten bekannt gewesen?
   a. Welche Maßnahmen hat der Informationssicherheitsbeauftragte unternommen, um diesen Missstand abzustellen?
   b. Wurde die ISK über diesen Missstand vom Informationssicherheitsbeauftragten informiert?
33. Wer war der jeweilige Informationssicherheitsbeauftragte seit Inbetriebnahme des EDIS?
34. Wie viele klassifizierte Schriftstücke, aufgeschlüsselt nach Eingangsstücken und Akten gesamt (InfoSiG, GehSO, PolKG) sind dort gespeichert?
   a. Wie viele sind eingeschränkt?
   b. Wie viele sind vertraulich?
   c. Wie viele sind geheim?
   d. Wie viele sind Streng geheim?
35. Wie viele klassifizierte Schriftstücke aufgeschlüsselt nach Eingangsstücken und Akten nach dem InfoSiG sind dort gespeichert?
   a. Wie viele sind eingeschränkt?
   b. Wie viele sind vertraulich?
   c. Wie viele sind geheim?
   d. Wie viele sind Streng geheim?
36. Wie viele klassifizierte Schriftstücke aufgeschlüsselt nach Eingangsstücken und Akten nach der GehSO sind dort gespeichert?
   a. Wie viele sind eingeschränkt?
   b. Wie viele sind vertraulich?

c. Wie viele sind geheim?
d. Wie viele sind Streng geheim?

37. Wie viele klassifizierte Schriftstücke aufgeschlüsselt nach Eingangsstücken und Akten nach dem PolKG sind dort gespeichert?
    a. Wie viele sind eingeschränkt?
    b. Wie viele sind vertraulich?
    c. Wie viele sind geheim?
    d. Wie viele sind Streng geheim?
38. Exemplarisch: Sind Informationen der CIA, des MI6, des MOSSAD, des BND, des HNaA, etc., die mit CONFIDENTIAL/VERTRAULICH, gekennzeichnet sind im EDIS gespeichert?
    a. Wenn ja, entspricht das dem InfoSiG?
    b. Wenn ja, entspricht dies der GehSO?
    c. Wenn ja, entspricht dies dem PolKG?
39. Exemplarisch: Sind Informationen der CIA, des MI6, des MOSSAD, des BND, des HNaA, etc., die mit SECRET/GEHEIM, gekennzeichnet sind im EDIS gespeichert?
    a. Wenn ja, entspricht das dem InfoSiG?
    b. Wenn ja, entspricht dies der GehSO?
    c. Wenn ja, entspricht dies dem PolKG?
40. Exemplarisch: Sind Informationen der CIA, des MI6, des MOSSAD, des BND, des HNaA, etc., die mit TOP SECRET/STRENG GEHEIM, gekennzeichnet sind im EDIS gespeichert?
    a. Wenn ja, entspricht das dem InfoSiG?
    b. Wenn ja, entspricht dies der GehSO?
    c. Wenn ja, entspricht dies dem PolKG?
41. Gibt es spezielle Aufbewahrungsvorschriften entsprechend des InfoSiG und werden/wurden diese durchgehend eingehalten?
42. Warum sind überhaupt so viele klassifizierte Informationen im EDIS gespeichert?
43. Wer ordnete diese Speicherungen an?
44. Seit wann erfolgten diese Speicherungen?
45. Wenn nein, warum müssen dann klassifizierte Dokumente über EDIS versendet werden oder wurden über EDIS versendet?
46. Stimmt es, dass andere Partnerdienste bezüglich der Verwendung ihrer Informationen belogen werden oder ihnen nicht die volle Wahrheit gesagt wurde?
47. Ist es möglich, Informationen von Partnerdiensten zu deklassifizieren, ohne deren Einverständnis einzuholen?
48. Wird diese Vorgangsweise im BVT praktiziert?
    a. Wenn ja, wer hat dies angeordnet?
    b. Seit wann erfolgt diese Vorgangsweise?
49. Ist es möglich, Informationen von Partnerdiensten durch Zusammenfassungen oder Umschreiben zu deklassifizieren?
50. Entspricht es der Wahrheit, dass der stellvertretende Direktor des BVT, Mag. Dominik FASCHING auf die Einhaltung der Gesetze betr. der Vertraulichkeit der Partnerdienstinformationen pocht und vom Direktor des BVT, Mag. Peter GRIDLING daran gehindert wird.?
51. Entspricht es der Wahrheit, dass es BVT Mitarbeitern mit Laptops möglich ist, via Fernzugriff („Tunnellösung") von überall aus der Welt auf das interne BVT-System und damit auch auf die im EDIS gespeicherten Partnerdienstinformationen ohne Einschränkung zuzugreifen?

a. Wenn ja, entspricht dies den gesetzlichen Vorgaben des InfoSiG?
b. Wenn ja, entspricht dies den gesetzlichen Vorgaben der GehSO?
c. Wenn ja, entspricht dies den gesetzlichen Vorgaben der PolKG?
d. Wenn ja, ist diese Praxis den Partnerdiensten bekannt?
e. Wenn ja, seit wann ist dies möglich?
f. Wenn ja, wer hat dies angeordnet?

52. Entspricht es der Wahrheit, dass es BVT Mitarbeitern mit Laptops möglich ist, via Fernzugriff („Tunnellösung") von jeder Polizeiinspektion/von jedem Polizeicomputer in Österreich auf das interne BVT-System und damit auch auf die im EDIS gespeicherten Partnerdienstinformationen ohne Einschränkung zuzugreifen?
    a. Wenn ja, entspricht dies den gesetzlichen Vorgaben des InfoSiG?
    b. Wenn ja, entspricht dies den gesetzlichen Vorgaben der GehSO?
    c. Wenn ja, entspricht dies den gesetzlichen Vorgaben der PolKG?
    d. Wenn ja, ist diese Praxis den Partnerdiensten bekannt?
    e. Wenn ja, seit wann ist dies möglich?
    f. Wenn ja, wer hat dies angeordnet?



2519

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2019-09-25T13:09:19+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.	