Bundesministerium
Verfassung, Reformen,
Deregulierung und Justiz

bmvrdj.gv.at

Dr. Clemens Jabloner
Bundesminister für Verfassung, Reformen,
Deregulierung und Justiz

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: BMVRDJ-Pr7000/0209-III 1/PKRS/2019

Ihr Zeichen: BKA - PDion (PDion)4160/J-NR/2019

Wien, am 11. November 2019

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Dr. Stephanie Krisper, Kolleginnen und Kollegen haben am 11. September 2019 unter der Nr. **4160/J-NR/2019** an mich eine schriftliche parlamentarische Anfrage betreffend „Vermeintlicher Hackerangriff auf die ÖVP" gerichtet.

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

Zur Frage 1:

- *Ist es korrekt, dass es eine Anzeige der ÖVP in diesem Zusammenhang gab?*
  a. Wenn ja: wann erfolgte die Anzeige und an welche Stelle erging diese?

Meinen Informationen zufolge erstattete die Österreichische Volkspartei (ÖVP) wegen des von ihr vermuteten und durch eigene Nachforschungen verifizierten Daten-Leaks im eigenen System am 5. September 2019 Anzeige beim Bundesministerium für Inneres (BMI).

Zur Frage 2:

- *Welche Organisationseinheiten des BMI sind mit den Ermittlungen in der Causa betraut?*
  a. Inwieweit ist das BVT in die Ermittlungen eingebunden?
  b. Sind Personen, die mit Ermittlungen im Zusammenhang mit der "Causa Ibiza" betraut sind, auch mit Ermittlungsaufgaben im Zusammenhang mit den hier skizzierten Sachverhalten rund um die mutmaßliche Cyberattacke auf die ÖVP-Server eingebunden?

i. Wenn ja: handelt es sich dabei auch um jene Personen, die laut Ihrem Interview in der ZIB 2 vom 27. August 2019, Mitglieder bei der ÖVP sind/waren?

Da diese Frage offenkundig in den Zuständigkeitsbereich des BMI fällt und ohnehin auch an den Herrn Bundesminister für Inneres gerichtet wurde, verweise ich in diesem Punkt mangels Ressortzuständigkeit auf dessen Anfragebeantwortung.

Zur Frage 3:

- *Auf Grund des Verdachts der Verletzung welcher strafgesetzlicher Normen wird in Bezug auf den "Cyber Incident" ermittelt? (Nennung der einzelnen Delikte des StGB)*

Das von der Staatsanwaltschaft Wien am 6. September 2019 eröffnete Ermittlungsverfahren wird derzeit gegen unbekannte Täter wegen des Verdachts des widerrechtlichen Zugriffs auf ein Computersystem (§ 118a Abs. 1 Z 2 StGB) und der Datenbeschädigung (§ 126a Abs. 1 StGB) zum Nachteil der ÖVP geführt.

Zur Frage 4:

- *Wird aufgrund der bekannt gewordenen Informationen zur "Buchhaltung" der ÖVP wegen Verletzung strafgesetzlicher Normen ermittelt? (etwa aufgrund § 163a StGB: Unvertretbare Darstellung wesentlicher Informationen über bestimmte Verbände oder anderen Delikten)*
  a. Wenn ja, aufgrund welcher Delikte genau wird gegen die ÖVP oder deren Funktionäre ermittelt und seit wann?

Nein.

Zu den Fragen 5 und 6:

- *5. Wurden seitens der ÖVP den Ermittler/innen wie angekündigt Beweismittel übergeben?*
  a. Wenn ja: wann und in welchem Ausmaß?
- *6. Wurde seitens der ÖVP, wie von Generalsekretär Nehammer medial verlautbart, den Ermittler/innen "voller Zugang zu allen Daten, allen Beweisen und allen Informationen in unserer Parteizentrale, die sie für die Aufklärung benötigen" gewährt?*
  a. Wurde diesem Angebot durch die Ermittler/innen bereits nachgekommen?
  b. Wenn nein: warum nicht?

Von den Vertretern der ÖVP wurden dem Bundesministerium für Inneres meinen Informationen zufolge Beweismittel für einen „Hackerangriff" in erheblichem Ausmaß vorgelegt. Zu welchem Zeitpunkt genau entzieht sich allerdings meiner Kenntnis. Die ÖVP hat jedenfalls den von ihr vor Anzeigeerstattung privat in Auftrag gegebenen, Datenleaks darstellenden Analysebericht an die Ermittlungsbehörden übergeben. Den Ermittlern wurde

auch Zugriff auf etwaige Protokolldateien und Analysesysteme gewährt. Ein technischer Experte der Ermittlungsgruppe ist zudem regelmäßig vor Ort und führt vor Ort Prüfungen durch.

Zur Frage 7:

- *Wurde seitens der ÖVP auch für die Ermittlungen in Zusammenhang mit der "Shredder-Affäre" bzw. der Causa Ibiza voller Zugang zu allen Daten, Beweisen und Informationen angeboten?*

Soweit mir bekannt ist, wurden der Staatsanwaltschaft Wien in der „Causa Ibiza" Beweise und Informationen angeboten, ein Zugang zu Daten erwies sich bislang allerdings als nicht erforderlich. In der „Schredder Affäre" zeigte sich der Beschuldigte kooperativ, ein weiterer Zugang zu Daten, Beweisen und Informationen war bislang aber ebenso wenig erforderlich.

Zu den Fragen 8, 9, 12 und 13:

- *8. Konnten die bisherigen Ermittlungsergebnisse den Verdacht eines Cyberangriffs auf die ÖVP-Parteizentrale erhärten (bitte um möglichst genaue Schilderung der Ermittlungsergebnisse und der daraus gezogenen Schlussfolgerungen)?*
- *9. Ist mittlerweile klar, welche Daten abgesaugt wurden?*
- *12. Ist der Zielserver der gestohlenen Daten bekannt und welche Rückschlüsse können aus dieser Erkenntnis auf den Urheber der mutmaßlichen Angriffe gezogen werden?*
- *13. Konnten Hinweise auf Datenmanipulation gefunden werden?*

Die bisherigen Ermittlungen bestätigen den Verdacht, dass sich ein unbekannter Täter ab dem 27. Juli 2019 Zugriff auf das gesamte ÖVP-IT-Netzwerk verschafft hat.

Aufgrund der bisherigen Untersuchungen ist weiters davon auszugehen, dass dieser unbekannte Täter zumindest eine Administrator-Passwortänderung im internen IT-Netzwerk der ÖVP durchgeführt hat. Damit wurden berechtigte Administratoren temporär aus der betroffenen EDV-Applikation der ÖVP ausgesperrt.

Außerdem wurde festgestellt, dass es jedenfalls zwischen 30. August 2019 und 1. September 2019 einen widerrechtlichen Datentransfer größeren Umfangs gegeben hat. Dabei wurden 463 Gigabyte auf einen französischen Zielserver übermittelt. Um welche Daten konkret es sich dabei handelt ist ebenso wie die Identifizierung der Person, die sich nach den bisherigen Erkenntnissen unberechtigt Zugriff auf das IT-System der ÖVP verschafft hat, Gegenstand der laufenden Ermittlungen.

Zu den Fragen 10 und 11:

- *10. Gibt es Hinweise, dass unter den abgesaugten Daten der ÖVP auch personenbezogene Daten iSd DSGVO waren?*
  a. Meldete die ÖVP bei der Datenschutzbehörde einen Data Breach gem Art 33 DSGVO?
    i. Wenn ja, wann genau und welchen Inhalt hatte die Meldung?
    ii. Erfolgte die Meldung fristgerecht innerhalb der gesetzlichen 72 Stundenfrist?
- *11. Fanden gesetzeskonform Benachrichtigungen der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person statt gem Art 34 DSGVO statt?*

Es wurde eine Meldung nach Art. 33 DSGVO erstattet. Diese langte am 5. September 2019 bei der Datenschutzbehörde ein. Der Inhalt der Meldung ist Gegenstand eines Verfahrens, das die Datenschutzbehörde gemäß Art. 52 DSGVO in völliger Unabhängigkeit zu führen hat. Es stehen mir daher auch keine weiteren Informationen zur Verfügung (vgl. § 19 Abs. 3 DSG).

Zu den Fragen 14 und 15:

- *14. Gibt es Hinweise darauf, dass es sich um einen Angriff eines ausländischen Geheimdiensts handelt?*
- *15. Gibt es Hinweise darauf, dass auch andere Parteien in vergleichbarem Ausmaß gehackt wurden bzw. dies versucht wurde?*

Nein.

Zu den Fragen 16 und 18:

- *16. Kann auf Grund der vorgelegten Unterlagen und der bisherigen Ermittlungsergebnisse ausgeschlossen werden, dass Daten aus der ÖVP, u.a. in Zusammenhang mit Parteispenden bzw. Wahlkampffinanzierung, durch einen "Maulwurf" in den eigenen Reihen (und nicht durch einen Cyberangriff) nach außen gespielt wurden (wenn ja: bitte um technische Erläuterungen, warum dies nach den vorgelegten Unterlagen ausgeschlossen werden kann.)*
- *18.Ist es denkbar, dass das Absaugen von Daten bzw. deren behauptete Manipulation in gar keinem ursächlichen Zusammenhang mit dem behaupteten Hack auf den Webserver stehen?*
  a. Ist es möglich, dass berechtigte Personen aus der ÖVP anonymisiert, selbst auf das Intranet zugegriffen und Daten kopiert haben oder diese Vorgänge durch Dritte durchführen ließen?
  b. Ist es möglich, dass Personen aus der ÖVP den "Angriff" auf den Webserver der ÖVP selbst durchführten oder durch Dritte durchführen ließen?

Wie bereits dargestellt, wird derzeit gegen unbekannte Täter ermittelt. Die Identifizierung der Person, die sich nach den bisherigen Erkenntnissen unberechtigt Zugriff auf das IT-System der

ÖVP verschafft hat, ist also Gegenstand der laufenden Ermittlungen. Als Justizminister ist es nicht meine Aufgabe, Spekulationen (etwa zu möglichen Tatbeteiligten) anzustellen.[1]

Zur Frage 17:

- *Gibt es Hinweise darauf, dass der Zugriff auf das Intranet der ÖVP im Zusammenhang mit den im Frühjahr dieses Jahres online abrufbaren Log-in Daten mehrerer Politiker (darunter Gernot Blümel) steht?*

Nein.

Zur Frage 19:

- *Gab es in der Vergangenheit Geschäftsbeziehungen des BMVRDJ bzw. seiner Organisationseinheiten und der CYBERTRAP Software GmbH bzw. der SEC Consult Unternehmensberatung (bitte um detaillierte Angaben zu Art und Umfang, beauftragende Stelle, Zeitraum etc.)?*

Nein.

Zur Frage 20:

- *Gibt es Hinweise, dass jene - laut ÖVP gefälschten - Mails, welche im Juni 2019 bekannt wurden (vgl. etwa https://www.derstandard.aUstorv/20001 05019335/kurz-und-ibiza-affaere-ein-email-skandal-der-keiner) und welche eine Beteiligung der ÖVP-Spitze am Ibiza Skandal nahelegen (sollten), auch auf Grund eines Hacks von Servern der ÖVP stammen?*

Nein.

Dr. Clemens Jabloner

[1] Beantwortung der dringlichen Anfrage, Frage 35 (S. 6 letzter Absatz).

REPUBLIK ÖSTERREICH BMVRDJ SIGNATUR	**Datum/Zeit**	2019-11-11T16:00:03+01:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: www.bmvrdj.gv.at/amtssignatur

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2019-11-19T17:17:02+01:00
	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.	