Bundesministerium
Inneres

bmi.gv.at

Dr. Wolfgang Peschorn
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: BMI-LR2220/0646-II/BK/5/2019

Wien, am 11. November 2019

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Dr. Stephanie Krisper, Kolleginnen und Kollegen haben am 11. September 2019 unter der Nr. **4161/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Vermeintlicher Hackerangriff auf die ÖVP" gerichtet, die ich nach den mir vorliegenden Informationen wie folgt beantworte:

Zu den Fragen 1 und 2:

- *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.*
- *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?*

Am 5. September 2019 erfolgte in diesem Zusammenhang eine Anzeige der ÖVP und wurde am selben Tag in der zuständigen Abteilung II/BK/5 des Bundeskriminalamtes eine Ermittlungsgruppe eingerichtet, welcher auch technische Experten des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung angehören.

Die Ermittlungen werden vom Bundeskriminalamt und nicht vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung geführt.

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)*

Die Ermittlungen werden unter Leitung der zuständigen Staatsanwaltschaft Wien wegen des Verdachtes gemäß § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem) und § 126a StGB (Datenbeschädigung) 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)*
  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:

- *Wurden seitens der ÖVP den Ermittler_Innen des BMI wie angekündigt Beweismittel übergeben?*
  a. *Wenn ja: wann und in welchem Ausmaß?*
- *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?*

Strafbehördliche Ermittlungsverfahren stehen unter der Leitung der Staatsanwaltschaften, deren Aufgaben die in den Wirkungsbereich des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz ressortieren. Von der ÖVP wurden den Ermittlungsbehörden ab dem 6. September 2019 Beweismittel in einem für die Ermittlungen zweckdienlichen Umfang zur Verfügung gestellt und Zugang zu den Informationen über die Datenverarbeitung gewährt.

Zu den Fragen 7 bis 9, 12 bis 14, 16, 18 und 20:

- *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?*
- *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)?*
- *Ist mittlerweile klar, welche Daten abgesaugt wurden?*
- *Ist der Zielserver der gestohlenen Daten bekannt und welche Rückschlüsse können aus dieser Erkenntnis auf den Urheber der mutmaßlichen Angriffe gezogen werden?*
- *Konnten Hinweise auf Datenmanipulation gefunden werden?*
- *Gibt es Hinweise darauf, dass es sich um einen Angriff eines ausländischen Geheimdiensts handelt?*
- *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.)*
- *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?*
- *Gibt es Hinweise, dass jene – laut ÖVP gefälschte – Mails, welche im Juni 2019 bekannt wurden (vgl. etwa https://www.derstandard.at/story/2000105019335/kurz-und ibiza-affaere-ein-e-mail-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?*

Im Hinblick auf das noch nicht abgeschlossene Ermittlungsverfahren und dessen Nichtöffentlichkeit (§ 12 StPO) ist eine Beantwortung dieser Fragen nicht zulässig. Das Ermittlungsverfahren steht unter der Leitung der Staatsanwaltschaften, die in den Wirkungsbereich des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz fallen, weswegen vom Bundesministerium für Inneres auch aus diesem Grund keine weiteren Informationen erteilt werden können.

Zu den Fragen 10 und 11:

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

In Österreich ist Aufsichtsbehörde nach § 33 DSGVO für die von einem Verantwortlichen im Sinne der DSGVO zu meldenden Vorkommnisse die weisungsfreie Datenschutzbehörde, die in den Wirkungsbereich des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz ressortiert.

Mangels Stellung als Verantwortlicher im Sinne des § 33 DSGVO und mangels Zuständigkeit zur Vollziehung des § 33 DSGVO kommt dem Bundesministerium für Inneres nach Art. 52 Bundes-Verfassungsgesetz in Verbindung mit§ 90 Geschäftsordnungsgesetz 1975 keine Zuständigkeit zur Beantwortung der obigen Fragen zu.

Zu den Fragen 15 und 17:

- *Gibt es Hinweise darauf, dass auch andere Parteien in vergleichbarem Ausmaß gehackt wurden bzw. dies versucht wurde?*
- *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?*

Entsprechende Hinweise gibt es nicht.

Zur Frage 19:

- *Gab es in der Vergangenheit Geschäftsbeziehungen des BMI 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.)?*

Mit der SEC Consult UB GmbH, etabliert in 2700 Wiener Neustadt, bestand im Jahr 2016 eine Vertragsbeziehung zum Zwecke der Durchführung einer Schulungsveranstaltung. Auf dieser Grundlage wurde am 25. und 26. Jänner 2016 eine Schulung zum Thema „Sichere Webanwendungen in der öffentlichen Verwaltung" abgehalten. Dafür wurde von der SEC

Consult UB GmbH der Republik Österreich der Betrag von EUR 6.000,-- (inkl. Steuern) in Rechnung gestellt.

Zu den Fragen 21 und 22:

- *Aus welchen Gründen wurde die Task Force „Hybride Bedrohungen" auf wessen Initiative installiert?*
- *Aus welchen Mitgliedern setzt sich diese zusammen?*

Am 29. September 2019 fand in Österreich die 27. Nationalratswahl statt.

In mehreren Staaten konnte in den vergangenen Jahren Versuche beobachtet werden, durch den Einsatz von hybriden Methoden und Mitteln verschiedener Akteure Einfluss auf Wahlen zu nehmen.

Die Einsetzung einer Task Force „Hybride Bedrohungen" wurde in einem Gespräch der Bundesminister für Landesverteidigung und des Bundesministers für Inneres am 10. Juli 2019 gemeinsam initiiert. Von den beiden Bundesministern wurde der Bundesregierung über die Absicht berichtet, mit der Einsetzung einer Task Force vorausschauend der denkmöglichen Gefahr einer Beeinflussung der Nationalratswahl 2019 zu begegnen. In weiterer Folge wurde die Task Force aus Experten des Bundeskanzleramts, des Bundesministeriums für Europa, Integration und Äußeres, des Bundesministeriums für Landesverteidigung sowie des Bundesministeriums für Inneres konstituiert. Auf Grundlage der Analysen und Empfehlungen dieser Experten wurden ab August 2019 spezifische Sicherungsmaßnahmen für die Durchführung der Nationalratswahl 2019 getroffen.

Durch die Mitwirkung der Experten aus den genannten Bundesministerien sollte sichergestellt werden, dass bestmöglich allen denkmöglichen hybriden Beeinflussungskampagnen auf die Nationalratswahl 2019 begegnet werden kann.

Zu den Fragen 23 und 24:

- *Welche Aufgaben kommen dieser zu?*
- *Inwieweit beschäftigt sich diese Task Force auch mit Vorfällen bei der ÖVP?*

Die Task Force „Hybride Bedrohungen" traf spezifische Maßnahmen, um die bevorstehende Nationalratswahl 2019 vor denkmöglichen Einflussnahmen durch hybride Methoden und Mitteln zu schützen. Die drei Hauptaufgaben waren:

- die Sicherstellung der physischen Cybersicherheit der IKT-Systeme innerhalb der Wahlinfrastruktur (Bundeswahl/Landeswahl/Gemeindewahlbehörden und die

Kommunikation zueinander, einschließlich Schwachstellenanalysen und Maßnahmen);

- die Beobachtung der Informationslage im Internet (z.B. Fake News) mit dem Ziel einer raschen Reaktion auf etwaige Beeinflussungsversuche;
- die intensive Kooperation mit dem Rapid Alert System auf EU-Ebene im Falle von Desinformationskampagnen;

Strafrechtliche Ermittlungstätigkeiten oblagen und obliegen der Task Force nicht.

Dr. Wolfgang Peschorn

	Datum/Zeit	2019-11-11T13:30:53+01:00
	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	2019-11-11T13:33:24+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.	