**4161/J XXVI. GP**

**Eingelangt am 11.09.2019**
**Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.**

# Anfrage

**der Abgeordneten Dr. Stephanie Krisper, Kolleginnen und Kollegen**

**an den Bundesminister für Inneres**

**betreffend Vermeintlicher Hackerangriff auf die ÖVP**

Am 5. September 2019 gab ÖVP-Parteiobmann Kurz bekannt, dass es zu einem Cyberangriff auf die ÖVP-Parteizentrale gekommen sei (https://www.derstandard.at/story/2000108265948/oevp-ortet-gross-angelegten-hackerangriff-auf-parteizentrale). Dabei sei eine große Anzahl an Daten entwendet bzw. manipuliert worden. Laut den beiden von der ÖVP mit der Überprüfung des behaupteten Hacks beauftragten Unternehmen "Cybertrap" und "SEC Consult" sei der Angriff seit 27. Juli 2019 erfolgt und habe bis 3. September 2019 angedauert. Als Vorbereitungszeit sei laut Zwischenbericht der SEC Consult eine Dauer von ein bis zwei Monaten anzusetzen.

Laut ÖVP ermitteln Beamt_Innen der Abteilung "Cyber Crime Competence Center" des Bundeskriminalamts in der Causa. Seitens der ÖVP wurde, wie man medialen Berichten entnehmen kann, auch zugesagt, sämtliche Ergebnisse und Beweise der in der Parteizentrale eingesetzten "Taskforce" dem Bundeskriminalamt zu übergeben. ÖVP-Generalsekretär Nehammer erklärte am 6. September 2019 überdies, den ErmittlerInnen "vollen Zugang zu allen Daten, allen Beweisen und allen Informationen in unserer Parteizentrale, die sie für die Aufklärung benötigen" zu gewähren (https://www.derstandard.at/story/2000108316063/oevp-kann-nicht-sagen-ob-geleakte-finanzdaten-gefaelscht-sind).

Die ÖVP konnte vorerst nicht sagen, ob die "geleakten" Daten zur Parteispendenaffäre bzw. zur Wahlkampffinanzierung verändert worden waren oder nicht, was insofern Fragen aufwirft, als laut Sicherheitsexperten "in einem Netzwerk quasi jeder Klick eine digitale Spur hinterlässt" und es daher "leicht feststellbar sein müsste, welche Dokumente abgesaugt oder manipuliert wurden". Laut IT-Sicherheitsexperten deutet einiges darauf hin, dass es bei der ÖVP "Versäumnisse in der IT-Security" gab (https://kurier.at/politik/inland/absolut-plausibel-was-experten-zum-hacker-angriff-auf-oevp-sagen/400597691).

Bemerkenswert in diesem Zusammenhang ist, dass erst im Mai 2019 bekannt wurde, dass Mailadresse und Passwort von Ex-Minister Blümel geleakt wurden und daher frei im Internet abrufbar waren (https://futurezone.at/netzpolitik/passwoerter-oesterreichischer-politiker-frei-im-netz-zugaenglich/400488727).

**Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.**

Eine weitere Frage, die sich in diesem Zusammenhang stellt, ist, in wie weit der behauptete Cyberangriff auf den Webserver und das Einloggen ins Intranet bzw. nachfolgende Absaugen von Daten zwingend in einem Zusammenhang stehen müssen, oder ob es sich dabei nicht auch um zwei von einander getrennte Aktionen handeln könnte. In anderen Worten: ist es auch denkbar, dass sich Personen aus der ÖVP mit entsprechenden Administratorenrechten anonymisiert im Intranet einloggten, um den Angriff durchzuführen.

Laut medialer Berichterstattung war der behauptete "Cyber-Incident" bei der ÖVP auch Thema der Beratungen der Task Force "Hybride Bedrohungen" (https://www.oe24.at/oesterreich/politik/wahl2019/oevp/OeVP-Attacke-Gipfel-mit-Geheimdiensten/396454969).

Die unterfertigten Abgeordneten stellen daher folgende

# Anfrage:

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?
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?
3. Auf Grund des Verdachts der Verletzung welcher strafgesetzlicher Normen wird in Bezug auf den "Cyber Incident" ermittelt? (Nennung der einzelnen Delikte des StGB)
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?
5. Wurden seitens der ÖVP den Ermittler_Innen des BMI 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?

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

   a. Wurde diesem Angebot durch die Ermittler_Innen bereits nachgekommen?
   b. Wenn nein: warum nicht?

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?
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?
10. 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 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?
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?
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?
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.)
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?
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?

**Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.**
www.parlament.gv.at

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.)?
20. Gibt es Hinweise, dass jene - laut ÖVP gefälschten - 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?
21. Aus welchen Gründen wurde die Task Force "Hybride Bedrohungen" auf wessen Initiative installiert?
22. Aus welchen Mitgliedern setzt sich diese zusammen?
23. Welche Aufgaben kommen dieser zu?
24. Inwieweit beschäftigt sich diese Task Force auch mit den Vorfällen bei der ÖVP?

**Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.**
www.parlament.gv.at