2986/J XXVII. GP

Eingelangt am 30.07.2020

Anfrage

der Abgeordneten Dr. Stephanie Krisper, Kolleginnen und Kollegen

an die Bundesministerin für Justiz

betreffend Stand des Verfahrens "Hackerangriff auf die ÖVP im Juli 2019"

Kurz nach Erscheinen eines Falterartikels mit dem Titel "Die geheime Buchhaltung der Liste Kurz" am 3. September 2019 gab ÖVP-Parteiobmann Kurz am 5. September 2019 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 Unternehmens "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. Der damalige 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).

Der Anfragebeantwortung 4156/AB durch den damaligen Bundesminister für Verfassung, Reformen, Deregulierung und Justiz DDr. Clemens Jabloner zu der schriftlichen Anfrage (4160/J) der Abgeordneten Dr. Stephanie Krisper, Kolleginnen und Kollegen an den Bundesminister für Verfassung, Reformen, Deregulierung und Justiz sowie der Anfragebeantwortung 4133/AB durch den Bundesminister für Inneres Dr. Wolfgang Peschorn zu der schriftlichen Anfrage (4161/J) der Abgeordneten Dr. Stephanie Krisper, Kolleginnen und Kollegen an den Bundesminister für Inneres betreffend Vermeintlicher Hackerangriff auf die ÖVP ist zu entnehmen:

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). Am selben Tag

wurde in der zuständigen Abteilung II/BK/5 des Bundeskriminalamtes eine Ermittlungsgruppe eingerichtet, welcher auch technische Experten des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung angehören.

Das von der Staatsanwaltschaft Wien am 6. September 2019 eröffnete Ermittlungsverfahren wurde 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.

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. Insbesondere wurde von der ÖVP der von ihr vor Anzeigeerstattung privat in Auftrag gegebenen, Datenleaks darstellenden Analysebericht an die Ermittlungsbehörden übergeben. Den Ermittler_innen wurde auch Zugriff auf etwaige Protokolldateien und Analysesysteme gewährt. Ein technischer Experte der Ermittlungsgruppe war zudem regelmäßig vor Ort und führte Prüfungen durch.

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

Laut Berichten der Wiener Zeitung richtete die Staatsanwaltschaft am 18. September 2019 darüber hinaus eine Ermittlungsanordnung an die französischen Behörden (https://www.wienerzeitung.at/nachrichten/politik/oesterreich/2030043-Ermittlungen-bestaetigen-Hackerangriff-auf-die-OeVP.html).

Seit Herbst 2019 war über den Ermittlungsstand in der Causa nichts mehr zu hören- was insofern verwundert, als der Nationale Sicherheitsrat der Bundesregierung mit öffentlichem Beschluss vom 11. September 2019 empfahl, jene ihr zur Verfügung stehenden Informationen betreffend des vermeintlichen Hackerangriffes auf die ÖVP mit der Öffentlichkeit zu teilen, die den Bürgerinnen eine auf Tatsachen gegründete Beurteilung der Situation ermöglichen.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Was ist der aktuelle Stand des Verfahrens?
2. Welcher Sachverhalt und konkreter Tathergang konnte mittlerweile festgestellt werden (um detaillierte Erläuterung wird ersucht)?
3. Auf Grund des Verdachts der Verletzung welcher strafgesetzlichen Normen wurde bis wann bzw. wird in Bezug auf den "Cyber Incident" noch ermittelt (um Antwort mit Nennung der einzelnen Delikte des StGB wird ersucht)?

4. Wurden die Ermittlungen hinsichtlich bestimmter Delikte eingestellt?
    a. Wenn ja, wann nach welchen Delikten und aus welchem Grund?
5. 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)?
6. Ist mittlerweile klar, welche Daten in welchem Ausmaß wohin genau abgesaugt wurden?
7. Konnten inzwischen bestimmte Täter ermittelt werden oder wird noch immer gegen"unbekannte Täter" ermittelt?
8. Ist der Zielserver der gestohlenen Daten bekannt und welche Rückschlüsse können aus dieser Erkenntnis auf den Urheber der mutmaßlichen Angriffe gezogen werden (um detaillierte Erläuterung wird ersucht)?
    a. Konnte die "Datenspur" ab dem französischen Server weiterverfolgt werden?
        i. Wenn ja, mit welchem Ergebnis wann?
        ii. Wenn nein, weshalb nicht? Woran scheiterte es?
9. Konnten konkrete Hinweise auf Datenmanipulation gefunden werden (um detaillierte Erläuterung wird ersucht)?
    a. Wenn ja, wann welche?
    b. Konnten hinsichtlich der im Falter veröffentlichten ÖVP-internen Dokumente Manipulation festgestellt werden?
        i. Wenn ja, welche genau wann?
10. 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)?
11. 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?
12. Welche Ermittlungshandlungen wurden seit Beginn der Ermittlungen jeweils wann durchgeführt (um detaillierte Erläuterung wird ersucht)?
13. Welche Beweise wurden jeweils wann erlangt (um detaillierte Erläuterung wird ersucht)?
14. Welche Ergebnis brachte die Ermittlungsanordnung an die französischen Behörden (um detaillierte Erläuterung wird ersucht)?
    a. Welchen Erkenntnisgewinn brachte die Ermittlungen in Frankreich?

15. Wurde das Ermittlungsverfahren mittlerweile abgeschlossen?
    a. Wenn ja, wann und zu welchem Schluss kommt die StA?
    b. Wenn ja, ist beabsichtigt, gegen einzelne oder mehrere der Beschuldigten Anklage zu erheben?
        i. Wenn ja, gegen wen?
        ii. Wann ist beabsichtigt, Anklage zu erheben?
    c. Wenn ja, wurden die Ermittlungen in der Causa eingestellt und aus welchen präzisen Gründen wann genau?
    a. Wenn nein, wann kann mit dem Abschluss der Ermittlungen gerechnet werden?
16. Wurden in der Causa Weisungen vom Ministerium oder der OStA Wien erteilt?
    a. Wenn ja, wann, von wem und mit welchem Inhalt?
17. Ist beabsichtigt, in der Causa Weisungen zu erteilen?
    a. Wenn ja, welche Weisungen beabsichtigen Sie in der Sache wann zu erteilen?
18. Wurde in der Causa ein Vorhabensbericht der StA erstattet?
    a. Wenn ja, mit welchem Inhalt/Vorhaben?
19. Wurde in der Causa eine Stellungnahme der OStA erstattet?
    a. Wenn ja, mit welchem Inhalt?
20. Wurden Ihnen bzw. dem Ministerium der Vorhabensbericht und die Stellungnahme bereits vorgelegt?
    a. Wenn ja: Wann wurden der Vorhabensbericht der StA und die Stellungnahme der OStA mit welchem Inhalt finalisiert?
21. Hat die StA vor, Anklagen gegen bestimmte Personen zu erheben?
    a. Wenn ja, gegen wen (bzw. wie viele Personen) wann und aufgrund welcher Delikte?
22. Hat die StA vor, das Verfahren gegen bestimmte Personen einzustellen?
    a. Wenn ja, gegen wen wann und mit welcher Begründung?