bmi.gv.at

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.141.869

Wien, am 30. März 2020

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Amesbauer und weitere Abgeordnete haben am 31. Jänner 2020 unter der Nr. **694/J** an mich eine schriftliche parlamentarische Anfrage betreffend „schwerwiegender Cyberangriff“ gerichtet.

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

Zur Frage 1:

- *Haben die Spezialisten, die aus Ihrem Ressort in dieser Angelegenheit aktiv sind, die Lage im Griff?*

Da es den Spezialisten des Bundesministeriums für Inneres nach intensiven Arbeiten und in hervorragender Zusammenarbeit mit Experten aller beteiligter Ressorts gelungen ist, die IT-Systeme des Bundesministeriums für Europäische und Internationale Angelegenheiten zu bereinigen und den Cyberangriff abzuwehren, ist davon auszugehen. Herr Bundesminister Mag. Alexander Schallenberg, LL.M., hat den involvierten Expertinnen und Experten seinen ausdrücklichen Dank für ihr großes Engagement und ihren Einsatz ausgesprochen und betont, dass sie in dieser schwierigen Situation Bemerkenswertes geleistet haben. Diesen aussagen kann ich mich nur anschließen.

Zu den Fragen 2 bis 11, 13, 15 und 16:

- *Wie lange konnten die Angreifer unbemerkt handeln, bis die Cyberattacke erkannt wurde?*
- *Wie viele und welche Daten wurden von den Angreifern bis zum Beginn der Abwehrmaßnahmen gehackt?*
- *Wie viele Spezialisten aus Ihrem Ressort wurden zu welchem Zeitpunkt des Angriffes für die Abwehr eingesetzt?*
- *Wie viele Spezialisten aus Ihrem Ressort sind für so einen Einsatz grundsätzlich vorhanden?*
- *Wie viele und welche Daten wurden während des gesamten Angriffes gehackt?*
- *Wurden sensible Daten gestohlen, die ein nachhaltiges Sicherheitsrisiko für die Republik Österreich darstellen?*
- *Sind Bürger von einem möglichen Datenabfluss betroffen?*
- *Wenn ja, in welcher Form und welchem Ausmaß ist das der Fall?*
- *Wenn ja, besteht für die betroffenen Bürger ein nachhaltiges Sicherheitsrisiko?*
- *Wer wird hinter dem Angriff vermutet?*
- *Gibt es einen Verdacht oder gar Erkenntnisse, welche konkreten Ziele die Angreifer mit dieser Attacke verfolgen?*
- *Wie hoch ist der zu erwartende Schaden?*
- *In welchen Bereichen ist der zu erwartende Schaden entstanden?*

Aufgrund der Verpflichtung zur Amtsverschwiegenheit, insbesondere im Interesse der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, sowie aus polizeitaktischen Gründen muss von einer Beantwortung dieser Fragen Abstand genommen werden.

In diesem Zusammenhang darf darauf hingewiesen werden, dass die Parlamentarische Kontrolle auch bei derartigen Vorfällen sichergestellt ist, indem sie einen Ständigen Unterausschuss des Ausschusses für Innere Angelegenheiten gemäß Art. 52 Bundes-Verfassungsgesetz eingerichtet hat. In diesem kann die Parlamentarische Kontrolle unter Wahrung der – für die Aufgabenerfüllung der Staatsschutzbehörden notwendigen, aber auch für den Schutz der Republik Österreich – Vertraulichkeit ausgeübt werden. Weiters hat sich der Nationale Sicherheitsrat mit der Angelegenheit beschäftigt.

Zur Frage 12:

- *Wer leitet die Ermittlungen?*

Am 7. Jänner 2020 erging ein Anfallsbericht vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung an die Staatsanwaltschaft Wien. Die Leitung dieses Ermittlungsverfahrens obliegt gemäß § 20 Strafprozessordnung der Staatsanwaltschaft Wien.

Zur Frage 14:

- *Besteht ein Zusammenhang mit den mutmaßlich im Sommer 2019 stattgefundenen Cyberangriffen auf die ÖVP-Zentrale?*

Zum gegenständlichen Zeitpunkt liegen keine Indizien vor, die auf einen möglichen Zusammenhang schließen lassen.

Zur Frage 17:

- *Welche Sicherheits- und Abwehrmaßnahmen sind notwendig, um das Risiko künftiger Attacken zu reduzieren?*

Das Bundesministerium für Inneres setzt – vor allem im präventiven Bereich – Maßnahmen, um die Cybersicherheit sowohl im staatlichen als auch im privaten Sektor zu erhöhen. Darüber hinaus sind im Regierungsprogram 2020 Maßnahmen definiert, die die weitere Stärkung der Cybersicherheit zum Ziel haben. Hierzu zählen vor allem die Schaffung eines staatlichen Cybersicherheitszentrums, die Stärkung der Zusammenarbeit mit Wissenschaft und Forschung aber auch Aus- und Fortbildungsmaßnahmen für IT-Spezialistinnen und -Spezialisten zur Schaffung von „Cyber Cops“ im Bundesministerium für Inneres.

All diese Maßnahmen verfolgen den Zweck und das Ziel, im Falle des Falles bestmöglich auf zukünftige Cybervorfälle vorbereitet zu sein und das Risiko künftiger Attacken auf die IT-Systeme von Bundesbehörden zu reduzieren.

Karl Nehammer, MSc

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2020-03-31T11:17:05+02:00
	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	2020-03-31T11:26:02+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.	