694/J XXVII. GP

Eingelangt am 31.01.2020

Anfrage

des Abgeordneten Amesbauer
und weiterer Abgeordneter
an den Bundesminister für Inneres
betreffend schwerwiegender Cyberangriff

In einer gemeinsamen Presse-Stellungnahme des BMEIA und des BMI wurde am 4. Jänner 2020 ein schwerwiegender Angriff auf die IT-Systeme des Außenministeriums bestätigt.

Diversen Medienberichten zufolge dauert der Angriff zumindest bis 17. Jänner 2020 an, vermutlich sogar darüber hinaus. Dass sogar die Assistenzleistung des Bundesheeres für die Abwehr dieser Cyberattacke angefordert werden musste, ist ein bislang einzigartiger Vorgang.

Aufgrund der beunruhigenden Medienberichte und mangels Informationen, weder an das Parlament noch an die Öffentlichkeit, sind die genauen Umstände und Hintergründe unbedingt aufzuklären.

In diesem Zusammenhang stellen die unterfertigten Abgeordneten an den Bundesminister für Inneres folgende

Anfrage

1. Haben die Spezialisten, die aus Ihrem Ressort in dieser Angelegenheit aktiv sind, die Lage im Griff?
2. Wie lange konnten die Angreifer unbemerkt handeln, bis die Cyberattacke erkannt wurde?
3. Wie viele und welche Daten wurden von den Angreifern bis zum Beginn der Abwehrmaßnahmen gehackt?
4. Wie viele Spezialisten aus Ihrem Ressort wurden zu welchem Zeitpunkt des Angriffes für die Abwehr eingesetzt?
5. Wie viele Spezialisten aus Ihrem Ressort sind für so einen Einsatz grundsätzlich vorhanden?
6. Wie viele und welche Daten wurden während des gesamten Angriffes gehackt?
7. Wurden sensible Daten gestohlen, die ein nachhaltiges Sicherheitsrisiko für die Republik Österreich darstellen?
8. Sind Bürger von einem möglichen Datenabfluss betroffen?
9. Wenn ja, in welcher Form und welchem Ausmaß ist das der Fall?

10. Wenn ja, besteht für die betroffenen Bürger ein nachhaltiges Sicherheitsrisiko?
11. Wer wird hinter dem Angriff vermutet?
12. Wer leitet die Ermittlungen?
13. Gibt es einen Verdacht oder gar Erkenntnisse, welche konkreten Ziele die Angreifer mit dieser Attacke verfolgen?
14. Besteht ein Zusammenhang mit den mutmaßlich im Sommer 2019 stattgefundenen Cyberangriffen auf die ÖVP-Zentrale?
15. Wie hoch ist der zu erwartende Schaden?
16. In welchen Bereichen ist der zu erwartende Schaden entstanden?
17. Welche Sicherheits- und Abwehrmaßnahmen sind notwendig, um das Risiko künftiger Attacken zu reduzieren?