

ENTSCHIESSUNGSAKTRAG

**der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen
betrifft Maßnahmen zur Herstellung der Verteidigungsfähigkeit im Cyberbe-
reich**

Von Dezember 2019 bis Anfang Februar 2020 fand ein gezielter und hochprofessioneller Cyberangriff auf das österreichische Außenministerium statt, dessen genaue Hintergründe und Urheberschaft aber noch weitgehend unbestätigt sind.

In den IT-Systemen eines der Schlüsselressorts der Republik operierte also über gerale Zeit hinweg ein feindliches System, hinter dem aufgrund des Umfangs, der zu Tage trenden Professionalität und der Resilienz der Malware, ein staatlicher bzw. staatsnaher Akteur zu stehen scheint. Am 13. Februar 2020 verkündete der Herr Außenminister, dass der Angriff beendet ist.

So erfreulich es ist, dass der Angriff auf das Außenministerium beendet werden konnte, so offenbarte er dennoch ernstzunehmende Schwachstellen in der Sicherheits- bzw. Verteidigungsarchitektur der Republik und beeinträchtigte die Integrität und Funktionsfähigkeit einer staatlichen Behörde und schadete damit der nationalen Sicherheit.

In einem Zeitalter, in dem die umfassende Digitalisierung auch in den Behörden stattfindet, hängt die nationale Sicherheit Österreichs maßgeblich von der Widerstands- und Verteidigungsfähigkeit der staatlichen Informationssysteme, klaren Behördenabläufen für Krisenfälle sowie von starken standardisierten Präventionsmaßnahmen ab.

Die unterfertigten Abgeordneten stellen daher folgenden

ENTSCHIESSUNGSAKTRAG

Der Nationalrat wolle beschließen:

"Die Bundesregierung wird aufgefordert,

1. die Urheber_innen und Hintergründe des Angriffs ausforschen und die aufgrund des Angriffes zutage getretenen Sicherheitslücken zu schließen,
2. zu überprüfen ob und inwieweit andere staatliche Behörden von gleicher oder ähnlicher Malware betroffen sind und gegebenenfalls entsprechende Maßnahmen zu setzen,

3. die allzeitige Verfügbarkeit von einsatzfähigen mobilen Elementen seitens des Bundesheeres sowie des Innenministeriums, jeweils mit ausreichender personeller und technischer Ausstattung und Know-How sicherzustellen,
4. in Zusammenarbeit mit den Bundesländern die organisatorischen wie technischen Rahmenbedingungen für Krisenfälle zu verbessern sowie
5. verbindliche Sicherheitsstandards hinsichtlich präventiver Vorkehrungen in staatlichen IT-Systemen auszuarbeiten."

In formeller Hinsicht wird die Zuweisung an den Ausschuss für innere Angelegenheiten vorgeschlagen.



