735/A(E)
vom 30.06.2020 (XXVII. GP)

ENTSCHLIESSUNGSANTRAG

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen betreffend Bericht über nationale Cybersicherheit

Seit dem hochprofessionellen Cyberangriff auf die Computersysteme des österreichischen Außenministeriums im Jänner 2020, der glücklicherweise abgewehrt werden konnte, ist klar, in welcher Intensität sich die Republik mittlerweile durch Cyberbedrohungen ausgesetzt sieht.

Der Angriff auf das Außenministerium offenbarte 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 sowie von starken standardisierten Präventionsmaßnahmen der staatlichen Informationssysteme und klaren Abläufen für Krisenfälle ab.

Cyberangriffe auf öffentliche oder private Organisationen stellen neben ihrer strafrechtlichen Relevanz insbesondere eine Gefahr für die Integrität der Demokratie und für unsere Gesellschaft dar. Die zuletzt erfolgte gezielte Cyberattacke gegen das Außenministerium mit dem Ziel der Informationsbeschaffung verdeutlicht diese Gefahr.

Dem genannten Angriff auf das Außenministerium gingen in den letzten Jahren bereits Angriffe auf andere staatliche Stellen sowie Einrichtungen der kritischen Infrastruktur voraus.

Mit dem Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), mit dem die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union umgesetzt wurde, erfolgte ein wesentlicher Schritt zur Verbesserung eines hohes Sicherheitsniveaus der Netz- und Informationssysteme.

In seinen Beschlüssen vom 28. Februar 2020 sprach der Nationale Sicherheitsrat gegenüber der Bundesregierung bereits diverse Empfehlungen aus.

So wurde der Bundesregierung unter anderem empfohlen:

1. die Urheber und Hintergründe des Angriffs bestmöglich aufzuklären und allfällig noch vorhandene Sicherheitslücken umgehend zu schließen,
2. zu überprüfen, ob und inwieweit andere staatliche Behörden von gleicher oder ähnlicher Malware betroffen sind,

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 und technischen Rahmenbedingungen für Krisenfälle zu verbessern sowie
5. verbindliche Sicherheitsstandards hinsichtlich präventiver Vorkehrungen in staatlichen IT-Systemen auszuarbeiten,
6. eine umfassende Evaluierung der Erfahrungen des Cyberangriffs auf das BMEIA und der Abwehr des Angriffs durchzuführen. Auf Basis dieser Evaluierung soll etwaiges Verbesserungspotential, insbesondere in den Bereichen Prozessmanagement, Personalbedarf sowie dem Aufbau von technischer und struktureller Infrastruktur, ausgearbeitet und bei Bedarf ein Reformprozess gestartet werden.

Dem Bundeskanzler sowie dem Innenminister kommen im Bereich der Netz- und Informationssystemsicherheit zentrale Aufgabe und Verantwortungen zu.

Aufgrund der umfassenden Bedeutung des Themas Cybersicherheit für die innere Sicherheit der Republik, ist es erforderlich, den gesetzgebenden Organen regelmäßig einschlägige Informationen über maßgebliche Entwicklungen zur Verfügung zu stellen, damit diese in den betreffenden Gremien erörtert werden können und die Aufgabenerfüllung der Regierung in diesem Bereich beurteilt werden kann.

Die unterfertigten Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

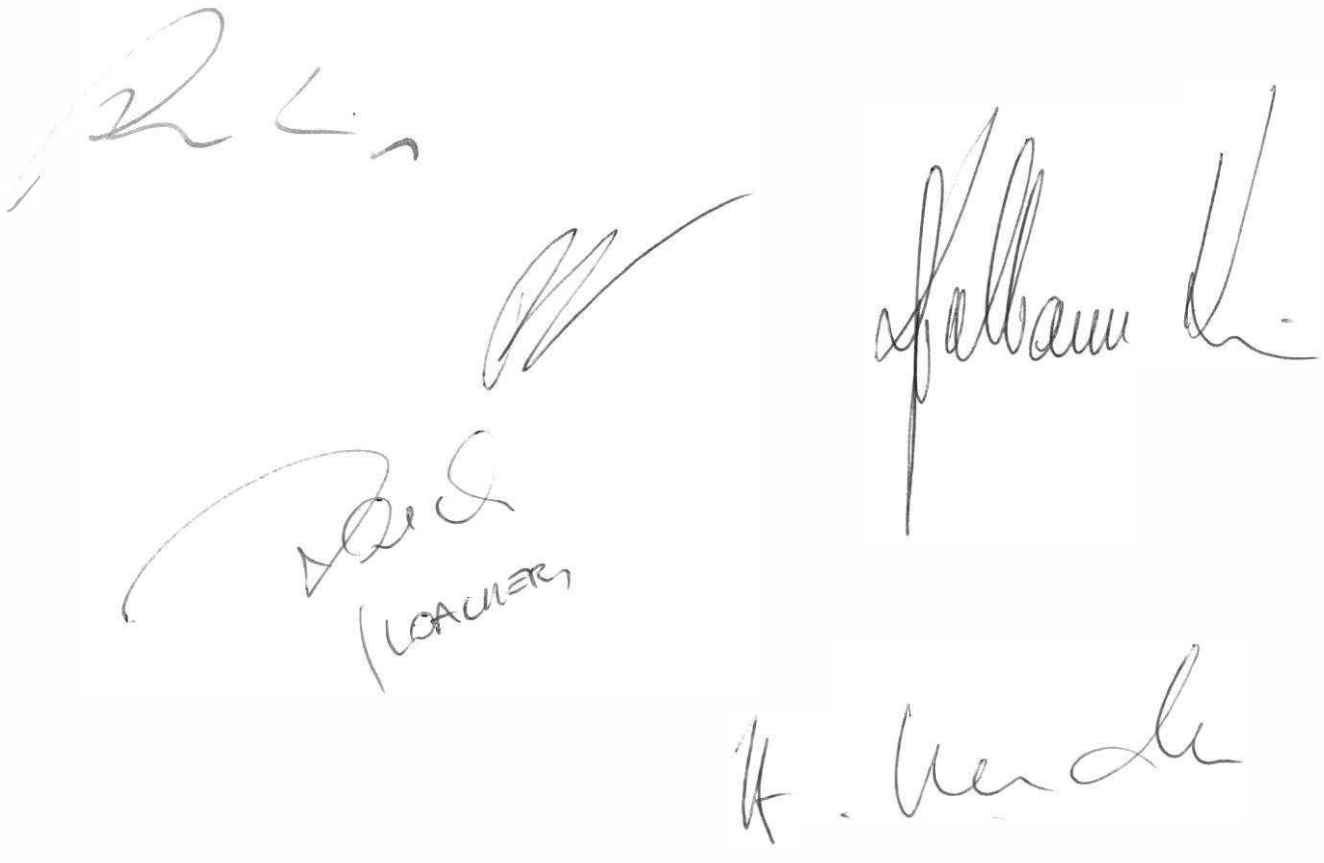
"Die Bundesregierung, insbesondere der Bundeskanzler, sowie der Bundesminister für Inneres, werden aufgefordert, dem Ständigen Unterausschuss des Ausschusses für Innere Angelegenheiten des Nationalrats jährlich einen Bericht über aktuelle und mögliche Cybersicherheitsbedrohungen mit Auswirkungen auf die nationale Sicherheit und die Wirtschaft der Republik Österreich vorzulegen.

Dieser Bericht soll insbesondere folgendes enthalten:

1. Eine aktuelle Analyse über die vorherrschenden Bedrohungslagen und Entwicklungen in Bezug auf Cybersicherheitsbedrohungen, einschließlich Cyberangriffe, Diebstahl und Datenschutzverletzungen, die gegen die Republik Österreich gerichtet sind und die nationalen Sicherheitsinteressen und die Wirtschaft der Republik Österreich bedrohen.
2. Angaben über die in diesem Bereich von den Bundesbehörden konkret gesetzten Aktivitäten zur Vorbeugung, Bewältigung und Abwehr solcher Cybersicherheitsbedrohungen.
3. Eine Bewertung der aktuellen Beziehungen der Republik Österreich zum Informationsaustausch und zur Zusammenarbeit mit anderen Ländern in Bezug auf Cybersicherheitsbedrohungen, einschließlich Cyberangriffe, Diebstahl und Datenschutzverletzungen, die gegen die Republik Österreich gerichtet sind und die nationalen Sicherheitsinteressen und die Wirtschaft der Republik Österreich bedrohen.

4. Eine Liste und eine Bewertung der Länder und nichtstaatlichen Akteure, die Hauptbedrohungen für die Cybersicherheit der Republik durch Cyberangriffe, Diebstähle oder Datenverletzungen darstellen.
5. Eine Bewertung neuer Technologien oder Fähigkeiten, die die Fähigkeit der Republik verbessern würden, Cybersicherheitsbedrohungen, einschließlich Cyberangriffe, Diebstahl und Datenschutzverletzungen, zu verhindern und darauf zu reagieren.
6. Eine Bewertung aller vom privaten Sektor verwendeten Technologien oder Praktiken, die schnell eingesetzt werden können, um die Behörden bei der Verhütung und Reaktion auf Cybersicherheitsbedrohungen zu unterstützen."

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



REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-07-04T20:16:43+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.	