366/A(E)
vom 27.02.2020 (XXVII. GP)

ENTSCHLIESSUNGSANTRAG

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen betreffend Stärkung der Forschung im Bereich Cybersicherheit

Am 4. Jänner 2020 hatte das Außenministerium einen gezielten und hochprofessionellen Cyberangriff gemeldet, der am 13. Februar 2020 offiziell als beendet erklärt wurde. Laut eines FM4-Berichts sei es den Angreifer_innen zwei Tage lang möglich gewesen, unbemerkt Zugriff auf die E-Mail-Server des Außenministeriums zu erlangen, Passwörter von Konten zu sammeln und Korrespondenzen zu exfiltrieren. Dass die Attacke in einer Frühphase entdeckt wurde, habe laut FM4 weniger mit Österreichs Cyberabwehr-Strategie als mit "einer Kombination aus günstigen Umständen, der Umsicht und Improvisationsfähigkeit der beteiligten Techniker sowie einem technischen Husarenstreich gegen die Kommunikation der Schadsoftware im Netz des Außenministeriums mit den externen Command-Control-Servern" zu tun (https://fm4.orf.at/stories/2998771/).

Dieser Cyberangriff auf das Außenministerium offenbart ernstzunehmende Schwachstellen in der Sicherheits- bzw. Verteidigungsarchitektur der Republik und beeinträchtigt die Integrität und Funktionsfähigkeit einer staatlichen Behörde. Doch auch andere Arten der Cyberkriminalität stellen ein ernstzunehmendes Problem für die staatliche und individuelle Sicherheit der Bürger_innen sowie für die Sicherheit von Unternehmen dar. Laut Cybercrime Report des Bundeskriminalamts aus dem Jahr 2018 hat die Zahl der Straftaten im Bereich der internetbasierten Kriminalität 2018 insgesamt 19.627 betragen. Das entspricht einer Steigerung um 16,8 Prozent im Vergleich zum Jahr 2017. Zum Vergleich: Im Jahr 2016 sind 13.103 solcher Delikte verzeichnet worden, 2015 nur 10.010. Die Zahl der Tatverdächtigen im Bereich der Internetkriminalität sei demnach 2018 um 7,1 Prozent im Vergleich zum Vorjahr auf 7.980 angestiegen. Massive Anstiege der angezeigten Fälle von Cybercrime (im weitest gedachten Sinne) wurden, bis auf Urkundenfälschungen (§§ 223 und 224 StGB), vor allem bei Erpressungen durch Ransomware (§§ 144 und 145 StGB) und bei pornografischen Darstellungen Minderjähriger im Internet (§ 207a StGB) verzeichnet.

Ohne konkrete Gegenmaßnahmen könne laut Bundeskriminalamt nicht mit einem Rückgang von Cyberkriminalität gerechnet werden. Begründet wird dies unter anderem mit der "Zunahme von vernetzten Endgeräten, IoT (Internet of Things) und dem Risiko des Einsatzes von (...) Machine Learning Algorithmen, welche sowohl zukünftige Angriffsflächen als auch Tatmittel und, damit verbunden, Angriffsdienstleistungen aus dem Darknet als Cybercrime as a Service (CaaS) wahrscheinlicher machen". Des Weiteren schließt das Bundeskriminalamt, dass "das Ausbreiten der Angriffe in schnelleren Wellen, mit einer größeren Anzahl an Geschädigten und höheren Schadenssummen" erfolgen werde. (https://bundeskriminalamt.at/306/files/Cybercrime_Report_18_web.pdf)

Umfangreiche Maßnahmen zur Eindämmung von Cyberkriminalität müssen daher ehestmöglich ergriffen werden. Dazu zählen allerdings nicht nur eine entsprechende Aufklärung der Bevölkerung und eine proaktive Verfolgung krimineller Online-Aktivitäten, sondern auch die intensive Erforschung und Entwicklung von Präventionsmaßnahmen sowie Abwehr- und Risikomanagement-Strategien. Die Einrichtung eines Lehrstuhls für Cybersicherheit und einer damit verbundenen Forschungsgruppe zum Thema "Security and Privacy" an der Technischen Universität Wien ist an dieser Stelle als positives Beispiel zu erwähnen, ebenso die IT-Sicherheit-Studiengänge an den Fachhochschulen Campus Wien und St. Pölten. Doch in Anbetracht der vielen düsteren Prognosen von Expert_innen - u.a. des renommierten Kaspersky Labs - wonach die Attacken auf unsere IT-Systeme immer ausgefeilter und spezifischer werden, ist es für den Schutz von kritischen Institutionen und Infrastrukturen sowie die Sicherheit der Bevölkerung unerlässlich, den Forschungsstandort Österreich im Bereich der Cybersicherheit finanziell und personell zu stärken und auszubauen.

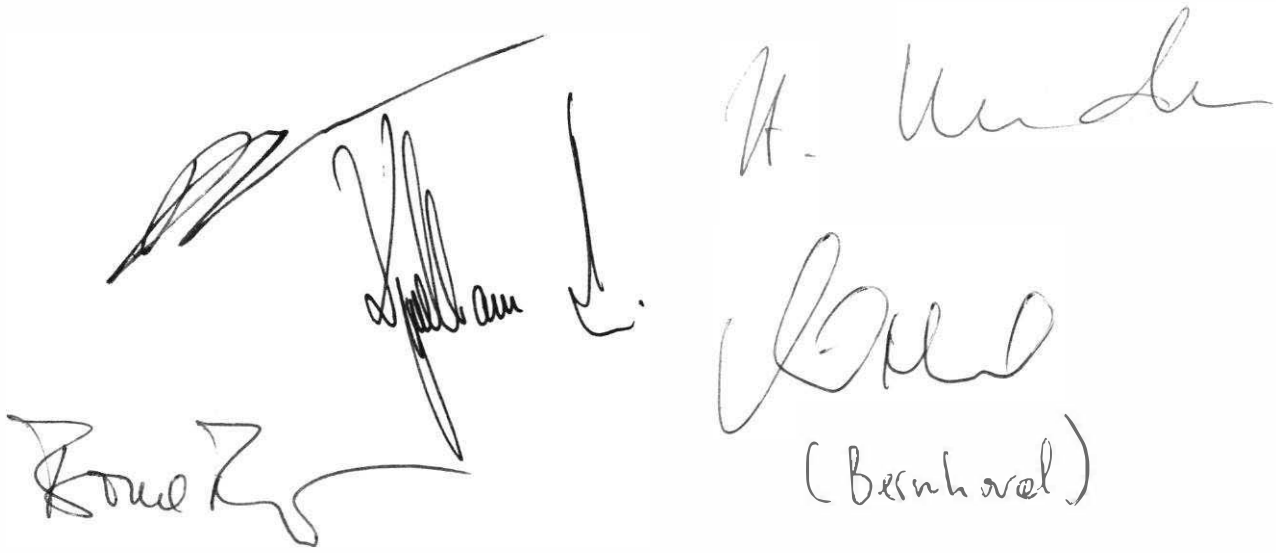
Die unterfertigten Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

"Die Bundesregierung, insbesondere der Bundesminister für Bildung, Wissenschaft und Forschung, wird aufgefordert, Grundlagen- und angewandte Forschung im Bereich Cybersicherheit zu stärken. Dies soll insbesondere durch die Schaffung von Exzellenzinitiativen und Exzellenzclustern unter Einbeziehung der wesentlichen österreichischen Förderinstitutionen in deren Konzipierung und Abwicklung erfolgen."

In formeller Hinsicht wird die Zuweisung an den Ausschuss für Forschung, Innovation und Digitalisierung vorgeschlagen.



REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-02-27T15:35:18+01:00
	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.	