3592/AB-BR/2021
vom 06.07.2021 zu 3880/J-BR

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Bundesrates
Dr. Peter Raggl
Parlament
1017 Wien

Geschäftszahl: 2021-0.404.522

Wien, am 6. Juli 2021

Sehr geehrter Herr Präsident!

Bundesrätin Korinna Schumann, Bundesrat Stefan Schennach, Genossinnen und Genossen haben am 6. Mai 2021 unter der Nr. **3880/J-BR** an mich eine schriftliche parlamentarische Anfrage betreffend „Zoom-Bombing – Aktuelle Gefahrenlage und Strategie der Behörden in Österreich“ gerichtet.

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

Zur Frage 1:

- *Ist Ihnen oder Ihrem Ministerium das Phänomen des hier subsumierend verwendeten Begriffs Zoom-Bombing bekannt?*
  - *a. Wenn ja: Wie viele Vorfälle, die sich darunter subsumieren lassen, sind dem Innenministerium bekannt?*
  - *b. Wenn ja: Werden diese Fälle verfolgt und wie?*
  - *c. Wenn ja: Wie reagiert das Innenministerium konkret auf derartige Vorfälle?*
  - *d. Wenn ja: Auf welchen Plattformen kam es zu derartigen Vorfällen?*
  - *e. Wenn nein: Wie erklären Sie, dass diese Art der Angriffe nicht bekannt sind?*

"Zoom-Bombing" ist ein Phänomen, das dem klassischen Cybercrime-Bereich zuzuordnen ist und dementsprechend auch im Rahmen der Sitzungen des Inneren Kreises der

Operativen Koordinierungsstruktur (IKDOK) nach Maßgabe der Bestimmungen des (Netz- und Informationssystemsicherheitsgesetz – NISG) thematisiert wurde.

Den österreichischen Sicherheitsbehörden sind sechs Tathandlungen, die sich unter dem Begriff "Zoom-Bombing" subsumieren lassen, bekannt. Dabei handelte es sich um vier staatsschutzrelevante, dem rechtsextremistischen Bereich zuordenbare Vorfälle sowie um zwei Fälle, bei denen im Zuge von Webinaren, die via ZOOM abgehalten wurden, durch einen Teilnehmer der sexuelle Missbrauch eines Kindes geteilt wurde. Diese Tathandlungen ereigneten sich größtenteils auf der anfragegegenständlichen Plattform ZOOM sowie auf dem Homeschooling/Videoportal des Tiroler Schulnetzes.

Es wurden bezüglich aller genannten Vorfälle Ermittlungen eingeleitet und entsprechende Anzeigen gelegt. Die weiterführenden strafbehördlichen Ermittlungsverfahren stehen unter der Leitung der Staatsanwaltschaft, der es als „dominus litis“ somit obliegt, über allfällige Ermittlungsschritte zu entscheiden. Um die nicht abgeschlossenen Ermittlungen im anfragegegenständlichen Zusammenhang nicht zum Nachteil der Strafrechtspflege zu beeinträchtigen und im Hinblick auf die Nichtöffentlichkeit des strafbehördlichen Ermittlungsverfahrens, wird von einer ausführlicheren Beantwortung Abstand genommen.

Zu den Fragen 2 bis 6, 10 und 11:

- *Führt das Innenministerium Statistiken hinsichtlich der Art der in Zoom-Meetings begangenen Übergriffe hinsichtlich ihrer Zielrichtung (rechtsextrem, antisemitisch, sexuell übergriffig etc.)?*
  - *a. Wenn ja: Wie teilen sich die Taten danach auf? Listen Sie diese bitte vollständig inklusive der Anzahl der bekannten Übergriffe auf*
  - *b. Wenn nein: Warum nicht?*
  - *c. Wenn nein: Ist angedacht, diesen Umstand in Zukunft zwecks besserer Ermittlungsstrategien zu ändern?*
- *Welche Maßnahmen sind vonseiten des Innenministeriums geplant, um zukünftig derartige Übergriffe zu verhindern?*
- *Gibt es Hinweise darauf, dass es besonders durch rechtsextreme und antisemitische Gruppierungen zu Zoom-Bombing kommt?*
- *Was wird das Innenministerium unternehmen, um möglichst viele Menschen die Zoom oder vergleichbare Plattformen nutzen, vor derartigen Übergriffen zu schützen bzw. diese davor zu wappnen?*
- *Ist die Kooperation mit anderen Ministerien, beispielsweise mit dem Bildungsministerium geplant, um auch in Schulen und Universitäten für den Schutz der NutzerInnen zu sorgen?*

   a. *Wenn ja: Wie gestalten sich diese Kooperationen?*
   b. *Wenn ja: Mit welchen Ministerien ist hier eine Kooperation bereits etabliert, mit welchen geplant?*
   c. *Wenn nein: Warum nicht?*
- *Welche Hilfe wird Opfern von Zoom-Bombing-Angriffen angeboten?*
- *Sind hinsichtlich einer österreichischen Szene Daten im Innenministerium vorhanden?*

Derzeit liegen den österreichischen Staatsschutzbehörden keine Hinweise bzw. Tendenzen vor, dass "Zoom-Bombing" im Besonderen durch rechtsextremistische und antisemitische Gruppierungen betrieben wird. Über die genannten Vorfälle und Erkenntnisse hinaus können mangels weiterer Erfahrungswerte mit Anzeigen und konkreten Opfern in diesem Zusammenhang, keine weiterführenden Informationen bereitgestellt werden. Es werden auch keine anfragespezifischen, in diverse Deliktsgruppen geteilte Statistiken geführt.

Eine Verhinderung von derartigen Übergriffen wäre nur durch umfassende Live-Zensur sämtlicher Videokonferenzen und sämtlicher Aktivitäten im Cyberraum zu erreichen. Ein solches Vorgehen steht jedoch im klaren Widerspruch zu den in der österreichischen Bundesverfassung und der EMRK garantierten Grund- und Freiheitsrechten.

Cybersicherheit ist in Österreich ein gesamtstaatliches Thema. Es handelt sich auch rechtlich um eine Querschnittsangelegenheit. Folglich gibt es keine Stelle, die österreichweit verbindliche Vorgaben geben kann. Aus diesem Grund ist eine starke Koordinierung und Bündelung von Kräften notwendig. Hauptzuständig sind neben dem Bundeskanzleramt das Bundesministerium für Inneres, das Bundesministerium für europäische und internationale Angelegenheiten sowie das Bundesministerium für Landesverteidigung.

Dabei koordiniert das Bundeskanzleramt nationale und internationale strategische Cybersicherheitsthemen und kooperiert in verschiedenen Arbeitsgremien mit nationalen, europäischen und internationalen Akteurinnen und Akteuren.

Im Bundesministerium für Inneres wurde im Jahre 2011 im Bundeskriminalamt das "Cybercrime Competence Center", kurz C4, zur Bekämpfung von Computer- und Internetkriminalität etabliert. Es ist die nationale und internationale Koordinierungs- und Meldestelle für Ermittlungen im Zusammenhang mit Cybercrime. Das C4 ist zudem für die elektronische Beweismittelsicherung und deren Auswertung zuständig und fungiert auch intern für alle heimischen und globalen Polizeidienststellen als wichtige Drehscheibe sowie Koordinationspunkt und gliedert sich mit ihren Schnittstellen zum Cyber Security

Center (CSC) des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung als wesentlicher Bestandteil in die Strategie des Bundeskanzleramts ein. Im Krisenfall erfolgt so die Unterstützung des "Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK)".

Die Experten in der Meldestelle im C4 sind rund um die Uhr jeden Tag im Einsatz. Sie sind rasche kompetente Ansprechpartner und stellen rasch und unkompliziert bei allen Fragen rund um Computer- und Internetkriminalität umgehend Verhaltenstipps und Erstmaßnahmen per E-Mail zur Verfügung. So kann im Schadensfall eine sofortige Unterstützung erfolgen. Eine Anzeigenerstattung muss im Schadensfall aber in einer Polizeiinspektion erfolgen.

Zu den Fragen 7 und 8:

- *Welche Abteilung ist im Innenministerium für die Verfolgung derartiger Angriffe zuständig und wie viele MitarbeiterInnen stehen dieser zur Verfügung?*
- *Gibt es vonseiten der Bundesregierung Pläne rechtliche Regelungen gegen derartige Übergriffe zu etablieren?*
  a. *Wenn ja: Bis wann ist mit einer Vorlage von Gesetzen an den Nationalrat zu rechnen?*
  b. *Wenn nein: Nach welchen Gesetzen werden derartige Angriffe verfolgt?*

Betreffend die spezifische Zuständigkeit zur Vornahme von weiteren Verfolgungshandlungen kann keine eindeutige Zuordnung getroffen werden, da je nach Vorfall verschiedene strafrechtliche Delikte verwirklicht wurden, deren Verfolgung wiederum unterschiedlichen Organisationseinheiten obliegen. Die konkrete Verfolgung in den vorliegenden Fällen erfolgte deliktsspezifisch im strafprozessualen Sinne.

Die Erteilung von darüber hinausreichenden Rechtsauskünften fällt nicht unter das parlamentarische Interpellationsrecht.

Zur Frage 9:

- *Stehen Sie mit Ihren AmtskollegInnen auf europäischer und internationaler Ebene in Kontakt um Strategien zur Bekämpfung des Zoom-Bombings voranzutreiben?*
  a. *Wenn ja: Wie sind die Fortschritte bei der Entwicklung dieser Strategien?*
  b. *Wenn ja: Bis wann ist mit konkreten Ergebnissen aus diesen Beratungen zu rechnen?*
  c. *Wenn nein: Warum nicht?*

Die Verwendung von ZOOM fand bei den Institutionen der Europäischen Union von Anfang an wenig Unterstützung. Die Europäische Kommission hat von ZOOM weitere Zusicherungen bezüglich der Sicherheit ihrer Technologie gefordert, nachdem Bedenken über die Datenschutzprotokolle des Unternehmens aufgetaucht waren. Da zudem im Oktober 2020 eine Sitzung des Rates für Auswärtige Angelegenheiten Ziel einer solchen Attacke durch einen niederländischen Reporter wurde, beläuft sich die derzeitige Strategie darauf, ZOOM nicht zu verwenden. Jedenfalls stand dieses Thema in letzter Zeit nicht auf der Agenda der Meetings auf EU-Ebene.

Karl Nehammer, MSc

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2021-07-06T16:09:18+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	148769640
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	2021-07-06T16:13:17+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.	