

Rudolf Anschober
 Bundesminister

Herrn
 Mag. Wolfgang Sobotka
 Präsident des Nationalrates
 Parlament
 1017 Wien

Geschäftszahl: 2020-0.223.004

Wien, 26.5.2020

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 1422/J des Abgeordneten Hoyos-Trauttmansdorff, Kolleginnen und Kollegen betreffend die Sicherheitslücke Zoom** wie folgt:

Fragen 1 bis 5:

- *Wurde bzw. wird der Zoom-Client für Windows in Ihrem Ministerium verwendet?*
 - a. *Wenn ja, wie viele Nutzer_innen verwenden diesen Client?*
 - b. *Wenn nein, welche Software wird für Videokonferenzen verwendet?*
- *Wurde bzw. wird Zoom über den Browser in Ihrem Ministerium verwendet?*
 - a. *Wenn ja, wie viele Nutzer_innen verwenden Zoom über den Browser?*
 - b. *Wenn nein, welche Browser-basierten Systeme werden für Videokonferenzen verwendet?*
- *War Ihnen diese "UNC path injection" Sicherheitslücke im Zoom-Client für Windows bekannt?*
 - a. *Wenn ja, haben Sie Maßnahmen ergriffen, um umgehend alternative Software zu verwenden? Welche?*
 - i. *Wenn nein, warum nicht?*
- *Ist Ihnen bekannt, ob durch diese Sicherheitslücke Windows Login-Daten gestohlen*

wurden?

a. Wenn ja, wie viele Nutzer_innen sind davon betroffen?

b. Welche Maßnahmen haben Sie ergriffen, um die Sicherheit der WindowsSysteme wiederherzustellen?

- *War Ihnen bekannt, dass Zoom-Calls - entgegen der Behauptungen des Anbieters - nicht end-to-end verschlüsselt werden?*

a. Wenn ja, haben Sie Maßnahmen ergriffen, um umgehend alternative Software zu verwenden? Welche?

i. Wenn nein, warum nicht?

Auf Grund von Sicherheitsbedenken wurde Zoom im Netzwerk des Ministeriums nicht freigegeben und wird daher nicht verwendet. Dies betrifft sowohl die Windows-Client- als auch die Browservariante.

Für Zwecke der Videokonferenzen ist auf den Windows-Geräten im Netzwerk des Ministeriums die Software GoToMeeting installiert.

Frage 6:

- *Wurden bzw. werden Tools für Videokonferenzen vor ihrem Einsatz auf ihre Sicherheitsstandards überprüft?*
 - a. Wenn ja, inwiefern?*
 - b. Wenn ja, durch wen?*
 - c. Wenn nein, warum nicht?*

Der Schutz der IKT-Systeme als auch personenbezogener Daten hat für das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz eine hohe Priorität. IKT-Sicherheit wird als fortlaufender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT - Sicherheitsstruktur vorgenommen. Bestehende und neue IKT-Lösungen werden in Zusammenarbeit durch das GovCERT als auch das Cyber Security Center des BMI fortlaufend evaluiert und Sicherheitslücken zeitnah adressiert. Systeme, die klassifizierte Informationen verarbeiten, werden im Rahmen eines Zulassungsprozesses (national, EU, NATO) auf deren Sicherheit überprüft.

Die Auswahl von IKT-Lösungen basiert auf konkreten Bedarfsanalysen, Sicherheitsanalysen und holistischen Betrachtungen des Application Lifecycles (Updates, Wartung, Ort der Datenverarbeitung und -speicherung, etc.).

Mit freundlichen Grüßen

Rudolf Anschober

