

1372/AB
vom 03.06.2020 zu 1423/J (XXVII. GP)
Bundesministerium bmkoes.gv.at
 Kunst, Kultur,
 öffentlicher Dienst und Sport

Mag. Werner Kogler
 Vizekanzler
 Bundesminister für Kunst, Kultur,
 öffentlichen Dienst und Sport

Herrn
 Präsidenten des Nationalrates
 Mag. Wolfgang Sobotka
 Parlament
 1017 Wien

Geschäftszahl: 2020-0.232.744

Wien, am 3. Juni 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 3. April 2020 unter der Nr. **1423/J** an mich eine schriftliche parlamentarische Anfrage betreffend Sicherheitslücke Zoom gerichtet.

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

Zu den 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 Windows Systeme wiederherzustellen?*
- *War Ihnen bekannt, dass Zoom-Calls - entgegen den 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?*

Lediglich zu Beginn des „Lockdowns“ kam bei Videokonferenzen vereinzelt auch Zoom zur Anwendung. Auf Grund der Sicherheitsbedenken wurde Zoom im Netzwerk des Ministeriums nicht freigegeben und wird daher nicht mehr 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, weiters wird z.B. auch CISCO empfohlen. In diesem Zusammenhang wurde auch ein Informationsschreiben an die Bediensteten meines Ressorts gerichtet, das Verwendungs- und Sicherheitshinweise für Videokonferenzen im Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport enthält. In diesen Sicherheitshinweisen wird aus datenschutzrechtlichen Bedenken ausdrücklich von der Verwendung von Zoom und MS Teams abgeraten.

Zu 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 Kunst, Kultur, öffentlichen Dienst und Sport 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 Bundesministeriums für Inneres

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.).

Mag. Werner Kogler

