1339/AB
vom 28.05.2020 zu 1426/J (XXVII. GP)

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

bmk.gv.at

Leonore Gewessler, BA
Bundesministerin

leonore.gewessler@bmk.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.222.733

. Mai 2020

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 3. April 2020 unter der **Nr. 1426/J** an mich eine schriftliche parlamentarische Anfrage betreffend Sicherheitslücke Zoom gerichtet.

Zu Frage 1:

- *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?*

Der Zoom Client wird im BMK nur für die Teilnahme an extern veranstalteten Konferenzen über Anforderung zur Verfügung gestellt. Derzeit ist der Zoom Client rund 500 PCs über die zentrale Softwareverteilung zugewiesen.
Standardmäßig wird Zoom für Videokonferenzen nicht verwendet, es stehen im BMK für Videokonferenzen Skype for Business, SIB-VC und eyeson zur Verfügung.

Zu Frage 2:

- *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?*

Die Anzahl der Nutzer_innen ist nicht bekannt. Standardmäßig werden SIB-VC und eyeson verwendet.

Zu Frage 3:

- *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?*

Wie schon in meiner Beantwortung zu Frage 1 ausgeführt, stehen für die Veranstaltung von Konferenzen eigene Lösungen zur Verfügung. Da aber eine Teilnahme an extern veranstalteten Zoom-Konferenzen erforderlich ist, kann für diesen speziellen Fall keine Alternative angeboten werden.

Zu Frage 4:

- *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?*

In meinem Ressort werden keine Zoom Accounts zur Verfügung gestellt. Für den Diebstahl von Windows Login-Daten gibt es keinerlei Hinweise. Daher waren bisher keine diesbezüglichen Maßnahmen erforderlich.

Zu Frage 5:

- *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?*

Die Schwachstellen von Zoom sind im Ressort bekannt, es werden daher primär alternative Systeme eingesetzt. Um bekannte Schwachstellen von Zoom rasch zu beseitigen, wird die Version des Zoom Clients laufend aktualisiert.

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?*

Grundsätzlich wird jede Software im Rahmen der Möglichkeiten des BMK vor ihrem Einsatz einer Basisüberprüfung unterzogen. Weitergehende Prüfungen bezüglich der IKT Sicherheit werden seitens des Bundeskanzleramtes vorgenommen. Sowohl der Schutz der IKT-Systeme als auch personenbezogener Daten hat für das Bundeskanzleramt 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 und 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.).

Leonore Gewessler, BA

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR KLIMASCHUTZ, UMWELT, ENERGIE, MOBILITÄT, INNOVATION UND TECHNOLOGIE
@ AMTSSIGNATUR

Hinweis	Dieses Dokument wurde amtssigniert.
Datum	2020-05-28T16:16:18+02:00
Seriennummer	1871969199
Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-05-28T18:11:17+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.	