1395/AB
vom 03.06.2020 zu 1419/J (XXVII. GP)

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.225.555

Wien, am 3. Juni 2020

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 3. April 2020 unter der Nr. **1419/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Sicherheitslücke Zoom“ gerichtet.

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

Zur Frage 1:

- *Wurde bzw. wird der Zoom-Client für Windows in Ihrem Ministerium verwendet?*
  a. *Wenn ja, wie viele NutzerInnen verwenden diesen Client?*
  b. *Wenn nein, welche Software wird für Videokonferenzen verwendet?*

Nein, der Zoom-Client für Windows wird nicht verwendet. Die Abhaltung von Videokonferenzen ist durch einen Erlass geregelt. Darin wird die ausschließliche Verwendung von „Skype for Business“ und die „Videokonferenzanlage (VKA)“ des Herstellers Cisco festgelegt.

Zur Frage 2:

- *Wurde bzw. wird Zoom über den Browser in Ihrem Ministerium verwendet?*
  a. *Wenn ja, wie viele NutzerInnen verwenden Zoom über den Browser?*

b. Wenn nein, welche Browser-basierten Systeme werden für die Videokonferenzen verwendet?

Nein, die Verwendung von Zoom im Browser wird technisch verhindert.

Die Regelung mittels Erlasses sieht vor, dass lediglich die auf allen Endgeräten (Desktop-PC, Notebook, iPhone und iPad) des BMI installierte „Software Skype for Business“ bzw. die „Videokonferenzanlage (VKA)“ des Herstellers Cisco zu verwenden ist. Die Nutzung anderer vom BMI nicht betreuter Kommunikationslösungen für dienstliche Zwecke (Browser-basiertes System) wird nicht unterstützt.

Zur 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?

Ja, die Sicherheitslücke im Zoom-Client für Windows war bekannt.

Zoom ist daher im BMI-Netzwerk für alle BenutzerInnen gesperrt. Eine Alternative musste wegen der bereits auf allen Endgeräten installierten Software „Skype for Business“ nicht angeboten werden.

Zur Frage 4:

- *Ist Ihnen bekannt, ob durch diese Sicherheitslücke Windows Login-Daten gestohlen wurden?*
  a. Wenn ja, wie viele NutzerInnen sind davon betroffen?
  b. Welche Maßnahmen haben Sie ergriffen, um die Sicherheit der Windows-Systeme wiederherzustellen?
  i. Wenn nein, warum nicht?

Im BMI wurden durch diese Sicherheitslücke keine Login-Daten gestohlen.

Zur 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?*

Ja, es war bekannt, dass Zoom-Calls keine End-to-end-Verschlüsselungen verwenden. Zoom ist daher im BMI-Netzwerk für alle BenutzerInnen gesperrt. Eine Alternative musste wegen der bereits auf allen Endgeräten installierten Software „Skype for Business“ nicht angeboten werden.

Zur 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?*

Die Videokonferenzsoftware „Skype for Business“ wird im BMI auf eigenen Servern im Rechenzentrum des BMI betrieben. Externe Teilnehmer werden über das „Skype for Business“-Service der Firma Microsoft eingeladen und umgekehrt.

Ebenso wird die „Videokonferenzanlage (VKA)“ der Firma Cisco auf BMI-eigener Infrastruktur betrieben. Auch hier können externe Teilnehmer über Cisco Services eingeladen werden.

Beide Systeme wurden aufgrund von öffentlich zugängigen bzw. von den Unternehmen zur Verfügung gestellten sogenannten White-Papers einer internen Sicherheitsbeurteilung unterzogen. Zusätzlich werden diese Systeme auch in wiederkehrenden externen Sicherheitsaudits überprüft.

Karl Nehammer, MSc

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2020-06-03T16:48:52+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1710479
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	2020-06-03T16:56:07+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.	