1359/AB
vom 03.06.2020 zu 1393/J (XXVII. GP)

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

bmdw.gv.at

Dr. Margarete Schramböck
Bundesministerin für Digitalisierung und Wirtschaftsstandort

buero.schramboeck@bmdw.gv.at
Stubenring 1, 1010 Wien

Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.222.234

Ihr Zeichen: BKA - PDion (PDion)1393/J-NR/2020

In Beantwortung der schriftlichen parlamentarischen Anfrage Nr. 1393/J betreffend "Sicherheitslücke Zoom", welche die Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen am 3. April 2020 an mich richteten, stelle ich fest:

Antwort zu den Punkten 1 und 2 der Anfrage:

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?*
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?*

In meinem Ressort steht auf jedem Arbeitsplatz Skype for Business mit Skype-Federations zu anderen Organisationen zur Verfügung. Wo die Nutzung von Skype aus Interoperabilitätsgründen nicht möglich ist, steht den Bediensteten die Nutzung der "Service im Bund Videokonferenzanlage" (SiB-VC) zur Verfügung, die im Bundesrechenzentrum betrieben wird und von jedem Ressort genutzt werden kann. SiB-VC bietet ein großes Maß an Interoperabilität. An SiB-VC Konferenzen kann mittels Skype, WebRTC-fähigen Browsern, Videoendpunkten oder Telefoneinwahl teilgenommen werden.

Daher musste nur in Fällen, in denen die Nutzung von Skype und/oder SiB-VC nicht möglich war, etwa weil mein Ressort nicht die einladende Organisation war, die Nutzung von

Konferenzlösungen wie GOTOMeeting, WebEx oder Zoom ermöglicht werden. So versenden etwa Internationale Organisationen wie die OECD Einladungen zu Zoom-Videokonferenzen. Deswegen wurde Mitte März 2020 die Installation des Zoom-Clients auf den IT-Arbeitsplätzen meines Ressorts durch die Benutzerinnen und Benutzer ermöglicht. Dabei wurden diese darauf hingewiesen, Zoom nur für nicht sensible Inhalte zu nutzen. Unmittelbar nach Bekanntwerden der ersten Sicherheitslücken im Windows Zoom-Client wurden die Installations- und Nutzungsmöglichkeit des Zoom-Clients deaktiviert und der Zoom-Client zentral von den IT-Arbeitsplätzen entfernt. Zum Zeitpunkt der zentralen Deinstallation war der Zoom-Client auf 106 von 980 Clients installiert. Alle Zoom-Client-Benutzerinnen und -Benutzer wurden über die Sicherheitsrisiken informiert. Die Teilnahme an Zoom-Konferenzen über kompatible Browser bleibt möglich.

Antwort zu den Punkten 3 bis 5 der Anfrage:

3. *War Ihnen diese "UNC path injection" Sicherheitslücke im Zoom-Client für Windows bekannt?*
    a. *Wenn ja, haben Sie Maßnahmen ergriffen, um umgehend altemative Software zu verwenden? Welche?*
        i. *Wenn nein, warum nicht?*
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?*
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 altemative Software zu verwenden? Welche?*
        i. *Wenn nein, warum nicht?*

Von den auch aus den Medien bekannten Schwachstellen in Zoom hat mein Ressort vom Computer Emergency Response Team der Europäischen Union (EU-CERT) sowie vom nationalen Government Computer Emergency Response Team (GovCERT) erfahren.

Meinem Ressort sind keine Data Breaches hinsichtlich gestohlener Windows Login-Daten aus der Zoom-Client-Schwachstelle bekannt. Benutzerinnen und Benutzer, die den Zoom-Client genutzt haben, wurden aufgefordert, ihr Passwort zu wechseln.

Im Übrigen ist auf die Antwort zu den Punkten 1 und 2 der Anfrage zu verweisen.

Antwort zu Punkt 6 der Anfrage:

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?

Eine risikogerechte Überprüfung der Sicherheitsstandards erfolgt für diese Tools; ebenso wie für IKT-Lösungen allgemein, wozu auf die Beantwortung der parlamentarischen Anfrage Nr. 1391/J durch den Herrn Bundeskanzler zu verweisen ist.

Wien, am 3. Juni 2020

Dr. Margarete Schramböck

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR DIGITALISIERUNG UND WIRTSCHAFTSSTANDORT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Digitalisierung und Wirtschaftsstandort
	Datum/Zeit	2020-06-03T06:54:39+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.	1237897311
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/. Die Bildmarke und Hinweise zur Verifikation eines Papierausdrucks sind auf https://www.bmdw.gv.at/amtssignatur oder http://www.help.gv.at/ veröffentlicht.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-06-03T07:01:48+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.	