1417/AB
vom 03.06.2020 zu 1414/J (XXVII. GP)

Bundesministerium
Bildung, Wissenschaft
und Forschung

bmbwf.gv.at

+43 1 531 20-0
Minoritenplatz 5, 1010 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.223.386

Die schriftliche parlamentarische Anfrage Nr. 1414/J-NR/2020 betreffend Sicherheitslücke Zoom, die die Abg. Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen am 3. April 2020 an mich richteten, wird wie folgt beantwortet:

Einleitend wird darauf hingewiesen, dass im Hinblick auf die mit der Digitalisierung einhergehende hohe Dynamik der Entwicklungen nur Momentaufnahmen wiedergegeben werden können. Digitale Lösungen werden von ihren Herstellern laufend weiterentwickelt. So wurde auch die in der gegenständlichen Parlamentarischen Anfrage angesprochene Sicherheitslücke mittlerweile geschlossen und das Videokonferenz-Tool angepasst.

Die zur Anwendung kommenden digitalen Lösungen werden seitens des Bundesministeriums für Bildung, Wissenschaft und Forschung einem regelmäßigen Monitoring unterzogen, um erforderlichenfalls unverzüglich Schritte setzen zu können. Alle Bereiche wurden und werden angewiesen, im Einsatz befindliche Softwarelösungen stets aktuell zu halten.

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?

In der Zentralstelle des Bundesministeriums für Bildung, Wissenschaft und Forschung wird einheitlich die Software Skype4Business (S4B) zur Verfügung gestellt (sowohl bei VPN-, als auch Citrixzugängen). S4B wird daher bevorzugt zur internen und externen Kommunikation verwendet. Alle Mitarbeiterinnen und Mitarbeiter wurden entsprechend angewiesen.

Nur in jenen Fällen, wo externe Organisationen zu einem Zoom-Meeting einladen, kommt der Zoom-Client zur Anwendung. Dieser ist nicht standardmäßig vorhanden, sondern kann von jeder Benutzerin bzw. jedem Benutzer zentral aus dem Softwarecenter selbständig installiert werden. Durch diesen Verteilungsmechanismus ist sichergestellt, dass immer die aktuellste Programmversion des Clients benutzt wird. Insgesamt 86 personenbezogene Installationen des Zoom-Clients sind auf den Arbeitsplatzgeräten erfasst. 60 Personen davon haben sich (via Webseite) als Zoom-Benutzer registriert.

Am überwiegenden Teil der Pädagogischen Hochschulen kommt Zoom in der serverbasierenden Pro-Version zum Einsatz. Dies erfolgt unter Einhaltung der in der Empfehlung des Bundesministeriums für Bildung, Wissenschaft und Forschung angeführten datenschutzrechtlichen Rahmenbedingungen.

Für den schulischen Bereich wird in den Empfehlungen des Bundesministeriums auf Microsoft Teams hingewiesen, das für Schülerinnen und Schüler und Lehrpersonen kostenlos im Office-365-Education Paket enthalten ist (https://www.bmbwf.gv.at/Themen/schule/beratung/corona/corona_fl/corona_ds.html).

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?

Eine Teilnahme an Videokonferenzen per Browser wird in der Zentralstelle des Bundesministeriums für Bildung, Wissenschaft und Forschung bevorzugt angeregt. Dazu werden über die zentrale Softwareverteilung mehrere moderne Browser zur Selbstinstallation angeboten. Grundsätzlich ist die Webseite von Zoom.us nicht zum Aufruf gesperrt. Da eine Teilnahme über den Browser eine Registrierung als Zoom-Benutzer voraussetzt, lässt sich eine Eingrenzung auf 60 Personen, die sich mit dienstlicher E-Mailadresse registriert haben, treffen.

Hinsichtlich der an den Pädagogischen Hochschulen zum Einsatz kommenden serverbasierenden Pro-Version wird bezüglich der Sicherheitsbedenken zur Konferenzsoftware Zoom auf die Empfehlungen des Bundesministeriums, abrufbar unter https://www.bmbwf.gv.at/Themen/schule/beratung/corona/corona_fl/corona_ds.html, hingewiesen.

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?

Der Fehler im Zoom-Client war durch Warnungen von Sicherheitsdienstleistern bekannt. Zusätzliche Maßnahmen waren nicht nötig, da einerseits der primäre Videodienst Skype4Business (S4B) ist, andererseits durch die zentrale Softwareverteilung ein aktualisierter Zoom-Client automatisch verteilt wurde.

Im Übrigen wird auf die vorstehenden Ausführungen zu Fragen 1 und 2 verwiesen.

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?

Die zugrundeliegende Windows Lücke wurde im Rahmen anderer Maßnahmen in der Infrastruktur unterbunden. Ein Login-Datendiebstahl auf diesem Wege kann daher nach jetzigem Wissensstand ausgeschlossen werden, sodass keine Personen betroffen waren. Nach Verfügbarkeit wurde der Zoom-Client im Rahmen des üblichen Patch-Managements umgehend auf allen Geräten auf den aktuellen Stand gebracht.

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 fehlende End-End Verschlüsselung wurde auch dem Bundesministerium für Bildung, Wissenschaft und Forschung bekannt. Grundsätzlich gilt für alle Multipunkt-Videokonferenzen, die keine Inhaltsverschlüsselung - sondern eine reine Transportverschlüsselung - aufweisen, dass eine vertrauenswürdige Mittlerstelle vorhanden sein muss. Dies gilt unabhängig vom eingesetzten Produkt.

Da es seitens der Zentralstelle des Bundesministeriums für Bildung, Wissenschaft und Forschung keine Empfehlung zum Einsatz des Zoom-Clients gegeben hat, sondern Skype4Business als Standard festgelegt ist, bestand kein Handlungsbedarf.

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 sowohl der IKT-Systeme als auch personenbezogener Daten hat für das Bundesministerium für Bildung, Wissenschaft und Forschung hohe Priorität. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur vorgenommen. Bestehende und neue IKT-Lösungen werden in Zusammenarbeit mit GovCERT und dem Cyber Security Center des Bundesministeriums für Inneres laufend evaluiert und Sicherheitslücken umgehend behoben. 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.).

Prinzipiell wird das Standardtool Skype4Business (S4B) verwendet. Für die Teilnahme an Videokonferenzen von Drittanbietern wird eine potentielle Clientsoftware zentral via Softwareverteilung bereitgestellt und im Rahmen des regulären Patch-Managements gepflegt. Generell wird versucht, möglichst alle Anforderungen über einen browserbasierenden Betrieb abzudecken und den Browser bestmöglich abzusichern.

Wien, 2. Juni 2020
Der Bundesminister:

Univ.-Prof. Dr. Heinz Faßmann eh.

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR BILDUNG, WISSENSCHAFT UND FORSCHUNG
@ AMTSSIGNATUR

Unterzeichner	Bundesministerium für Bildung, Wissenschaft und Forschung
Datum/Zeit	2020-06-03T18:36:02+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.	285175223
Hinweis	Dieses Dokument wurde amtssigniert.
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at. Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bmbwf.gv.at/verifizierung.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-06-03T18:43:22+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.	