506/A(E) XXVII. GP

Eingebracht am 28.04.2020

ENTSCHLIESSUNGSANTRAG

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

betreffend Sicheres Tool für Videokonferenzen in den Ministerien

Aufgrund der Covid-19-Pandemie steigt die Zahl der Nutzer_innen der Zoom-App zur Abhaltung von Videokonferenzen rasant an. Angaben des Unternehmens zufolge benutzen dieses Tool mittlerweile täglich ca. 300 Millionen Menschen weltweit, sowohl für private, als auch berufliche Zwecke. Expert_innen und Medienberichten zufolge gibt es bei der Verwendung von Zoom allerdings erhebliche Sicherheits- und Datenschutzbedenken.

Laut Datenschutzerklärung (Stand 27.3.2020) sammelt Zoom, unabhängig davon, ob ein Account angelegt wurde oder nicht, eine Vielzahl personenbezogener Daten, darunter Namen, Nutzernamen, Adresse, E-Mail Adresse, Telefonnumer, Berufsbezeichnung, Arbeitgeber, Kreditkarteninformationen, IP-Adresse, Betriebssystem und weitere Nutzungsdaten. Wird die Anwendung mittels Facebook-Login verwendet, werden auch Facebook-Profildaten gesammelt.

Auch über Sicherheitsbedenken wurde in den vergangenen Wochen gehäuft berichtet, für manche wurde bis dato keine Lösung gefunden. So ist der Zoom-Client für Windows anfällig für sogenannte "UNC path injection", die es Angreifer_innen ermöglicht, Login-Daten für die Windows-Systeme der Zoom-Anwender_innen zu stehlen. Um die Login-Daten zu stehlen, müssen Angreifer_innen lediglich gefälschte URLs über das Chat-Interface der App an die Zoom-Nutzer_innen senden, die in weiterer Folge nur einmal auf diesen Link klicken müssen (https://thehackernews.com/2020/04/zoom-windows-password.html). Da es noch keinen Patch für diese Schwachstelle des Zoom-Clients gibt, wurden Nutzer_innen angehalten, auf ein alternatives Tool auszuweichen oder Zoom über den Browser zu verwenden.

Weiters wurde bereits im März bekannt, dass Zoom-Calls entgegen der Behauptungen des Unternehmens nicht end-to-end verschlüsselt werden, sondern mittels Transportverschlüsselung. Das bedeutet, das Unternehmen kann auf die unverschlüsselten Video- und Audiodateien des Zoom-Meetings zugreifen. Diese Daten können so unter anderem an Regierungen oder die Exekutive weitergegeben werden - im Gegensatz zu anderen Unternehmen wie Google oder Microsoft veröffentlicht Zoom jedoch keinen Transparenzbericht darüber, wie oft Daten von Nutzer_innen

tatsächlich übermittelt wurden (https://theintercept.com/2020/03/31/zoom-meeting-encryption/).

Die Liste der sicherheitsrelevanten Zwischenfälle lässt sich fortsetzen: Mitte März deckten Sicherheitsforscher_innen massive, verdeckte Datenweitergaben an Facebook auf; "Zoom-Bombing", also die Störung von fremden Zoom-Meetings, hat sich mittlerweile zu einem ernstzunehmenden Problem entwickelt.

Auch zum Firmenstandort ergeben sich Fragen. So berichtete das kanadische "Citizen Lab" Anfang April, dass die Zoom-Headquarters zwar in den USA seien, die App selbst jedoch hauptsächlich von drei Unternehmen in China ("Ruanshi Software") entwickelt werde. Zwei dieser Unternehmen besitzt Zoom, das dritte dürfte ein Joint-Venture sein ("American Cloud Video Software Technology Co., Ltd."). 700 Mitarbeiter_innen beschäftigt das Unternehmen in China im Bereich F&E. Druck der chinesischen Regierung bzw. Behörden auf das Unternehmen wird daher befürchtet (https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/).

Unternehmen wie SpaceX und Google haben ihren Mitarbeiter_innen die Nutzung von Zoom aufgrund von Sicherheits- und Datenschutzbedenken bereits untersagt, ebenso die US-amerikanische Raumfahrtbehörde NASA.
Mitte April hat das Bundesministerium für Bildung, Wissenschaft und Forschung von der Verwendung von Zoom an Schulen abgeraten.

Die unterfertigten Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

"Die Bundesregierung, insbesondere die Bundesministerin für Digitalisierung und Wirtschaftsstandort wird aufgefordert, für die Abhaltung von Videokonferenzen in sämtlichen Ministerien anstelle der Zoom-App geeignete alternative Open-Source Anwendungen zu verwenden, die end-to-end verschlüsselte Gespräche ohne überschießende Nutzerdatensammlung bzw. -speicherung ermöglichen."

In formeller Hinsicht wird die Zuweisung an den Ausschuss für Forschung, Innovation und Digitalisierung vorgeschlagen.