

Anfrage

**der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen
an den Bundeskanzler**

betreffend Sicherheitslücke Zoom

Die Covid-19 Pandemie ließ die Nachfrage nach effizienten Tools für Videokonferenzen rasant steigen. Aufgrund der unkomplizierten Funktionsweise stieg insbesondere die Zahl der Nutzer_innen der "Zoom" App um ein Vielfaches, mehrere Millionen Menschen weltweit benutzen dieses Tool mittlerweile für Videochats. Medienberichten zufolge gibt es allerdings Bedenken hinsichtlich der Sicherheit der App für Windows-Nutzer_innen. 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.

Insbesondere in Anbetracht der Tatsache, dass dies nicht der erste sicherheitsrelevante Zwischenfall mit Zoom ist (Zoom-Calls werden unter anderem nicht end-to-end verschlüsselt <https://theintercept.com/2020/03/31/zoom-meeting-encryption/>), stellen sich Fragen zur Software, die im Bundeskanzleramt für Videokonferenzen verwendet wird.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Wurde bzw. wird der Zoom-Client für Windows im Bundeskanzleramt 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 im Bundeskanzleramt verwendet?
 - a. Wenn ja, wie viele Nutzer_innen verwenden Zoom über den Browser?
 - b. Wenn nein, welche Browser-basierten Systeme werden für Videokonferenzen verwendet?
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?
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 alternative Software zu verwenden? Welche?
 - i. Wenn nein, warum nicht?
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?

feil prüfung

Künzler

gallus k





