

## Anfrage

**der Abgeordneten Univ.-Prof. Dr. Alfred J. Noll, Stephanie Cox, BA,  
Kolleginnen und Kollegen,**

**an den Bundesminister für Verfassung, Reformen, Deregulierung und Justiz  
betreffend Bundestrojaner im „Digitalen Amt“?**

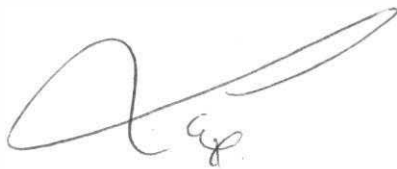
Vor Kurzem stellte die Regierung die Online-Plattform „oesterreich.gv.at“ und die Smartphone App „digitales Amt“ vor, mit denen die Abwicklung Behördenwege einfacher möglich sein sollen. Bürger, die diese App nutzen, teilen dort zahlreiche sehr sensible Daten (Mailadresse, Handynummer, Postleitzahl, „Auswahl interessanter Lebenslagen“, ...). Um die App vom Handy aus voll nutzen zu können, ist sogar eine Face- oder Touch-ID (Gesichtserkennung oder Fingerabdruck) notwendig.

Im Jahr 2018 wurde das sogenannte Sicherheitspaket (treffender: „Überwachungspaket“) beschlossen (BGBl I Nr 27/2018), das derzeit vom Verfassungsgerichtshof überprüft wird. Das Überwachungspaket ermöglicht unter anderem die Überwachung verschlüsselter Nachrichten mittels Installation einer Schadsoftware („Bundestrojaner“) auf den Smartphones der BürgerInnen. Die diesbezüglichen Bestimmungen treten mit 01.04.2020 in Kraft (vgl § 514 Abs 37 StPO) und fallen somit zeitlich eng mit der der Einführung des „Digitalen Amtes“ zusammen. Fraglich ist, wie es um die IT-Sicherheit des „digitalen Amtes“ bestellt ist, und ob dieses bereits Sicherheitslücken (so genannte „backdoors“) enthalten könnte. Aus ökonomischer Sicht hätten solche vorinstallierten „backdoors“ den Vorteil, dass das Wissen um Sicherheitslücken in anderen Programmen nicht teuer am Schwarzmarkt durch Strafverfolgungsbehörden zugekauft werden müsste. Bereits jetzt gibt es Sicherheitsbedenken gegen die App, weil sie in vielen Fällen nur eine Verlinkung auf Webseiten ist. Als Folge werden Daten über offene HTML-Ports übermittelt und können leicht ausgelesen werden.

Deshalb stellen die unterfertigten Abgeordneten folgende Anfrage:

1. Ist in Zukunft geplant, die App „digitales Amt“ als Einfallstor für Schadsoftware iSd „Bundestrojaners“ heranzuziehen?
  - a. Wenn ja: Inwiefern?
  - b. Wenn nein: Würden Sie uns darüber informieren, wenn dem so wäre?
  
2. Gab es bei der Programmierung dieser App eine Kooperation zwischen BMVRDJ und BMDW?
  - a. Wenn ja: Inwiefern?

- b. Wenn ja: Wurde dabei auch über die Nachrichtenüberwachung bzw die Überwachung verschlüsselter Nachrichten oder Schadsoftware gesprochen?
      - i. Wenn ja: Inwiefern?
    - c. Wenn ja: Was war das Ergebnis?
3. Ist die Kommunikation zwischen App und Server eine Nachricht iSd § 134 Z 3 StPO bzw § 134 Z3a StPO?
4. Wurden auch Experten aus dem Bereich des Datenschutzrechts konsultiert?
  - a. Wenn ja: Inwiefern?
  - b. Wenn nein: Weshalb nicht?

  
(Cox)

N  
— 4



Zu



