
3334/J XXVI. GP

Eingelangt am 16.04.2019

Dieser Text ist elektronisch textinterpretiert. Abweichungen vom Original sind möglich.

Anfrage

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

**an die Bundesministerin für Digitalisierung und Wirtschaftsstandort
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. Wurden bei der Programmierung der App Sicherheitslücken offen gelassen, über die es technisch möglich ist, Schadsoftware, wie etwa den „Bundestrojaner“ in das Endgerät einzuspielen?
 - a. Wenn ja: Welche?
 - b. Wenn nein: Würden Sie uns darüber informieren, wenn dem so wäre?

Dieser Text ist elektronisch textinterpretiert. Abweichungen vom Original sind möglich.

2. Weshalb wurde diese die App nicht als Open-Source-Software erstellt?
3. Sind Ihnen derzeit andere Sicherheitslücken der App bekannt?
 - a. Wenn ja: Welche?
 - b. Wenn ja: Was werden Sie tun, um diese Sicherheitslücken zu schließen?
 - c. Wenn ja: Werden diese Sicherheitslücken in Zukunft bewusst offen gelassen werden?
 - i. Wenn nein: Würden Sie uns darüber informieren, wenn dem so wäre?
4. 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?
5. 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?
6. Gab es im Zuge der Erstellung der Plattform oder der App eine Kooperation mit anderen Ministerien?
 - a. Wenn ja: Mit welchen?
7. In der Fragestunde vom 28.3.2019 sagte BM Schramböck, dass Experten der TU Graz, A-Sit und Egiz zu Sicherheitsaspekten des „digitalen Amtes“ herangezogen wurden.
 - a. Welche Bedenken äußerten die Experten?
 - b. Inwiefern wurden die Bedenken dieser Experten berücksichtigt?
 - c. Welche Bedenken dieser Experten wurden in der Umsetzung nicht berücksichtigt?
 - d. Erstellten diese Experten einen Bericht?
 - i. Wenn ja: Was waren die wesentlichen Ergebnisse dieses Berichts?
 - ii. Wenn ja: Werden Sie diesen veröffentlichen?
 1. Wenn nein: Weshalb nicht?
 - iii. Wenn nein: Weshalb nicht?

8. Wurden auch Experten aus dem Bereich des Datenschutzrechts konsultiert?
 - a. Wenn ja: Inwiefern?
 - b. Wenn nein: Weshalb nicht?

9. Wieviel kostete die App und die damit verbundenen Aktivitäten, zB Werbemaßnahmen von Beginn der Planung bis zur tatsächlichen Einführung (bitte um Aufstellung nach einzelnen Posten)?
 - a. Aus welchem Detailbudgets wurden diese Kosten beglichen?
 - b. Wo wurden Plattform und App beworben (Bitte Aufstellung nach Websites, Magazinen uä)?

10. Welche Vertragspartner haben bei der Erstellung der App mitgewirkt?
 - a. Welche Vertragsleistungen haben die einzelnen Vertragspartner erfüllt?
 - b. Über welchen Zeitraum wurden die einzelnen Vertragsleistungen erfüllt?
 - c. Nach welchen Kriterien wurden diese Vertragspartner ausgewählt?
 - d. Wurden die Leistungen öffentlich ausgeschrieben?
 - i. Wenn ja: Inwiefern?
 - ii. Wenn nein: Weshalb nicht?

11. Für den Zugriff auf die App benötigt man Face- oder Touch-ID. Für den Zugriff via Computer nicht. Inwiefern ist diese Differenzierung sachgerecht?
 - a. Welche anderen Unterschiede im Zusammenhang mit Zugriffsmöglichkeiten und Sicherheitsmaßnahmen gibt es zwischen Handy und Computer?
 - b. Inwiefern ist geplant, diese unterschiedlichen Sicherheitsmaßnahmen zu vereinheitlichen?

12. Welche konkreten Maßnahmen wurden gesetzt, um eine DSGVO-konforme Umsetzung der App und der Plattform zu gewährleisten?
 - a. Welche Daten sammeln die App und Plattform in Bezug auf die End-User?
 - b. Inwiefern hat die App oder die Plattform Zugriff auf die Daten, die durch Face- oder Touch-ID erhoben werden?
 - c. Welche sensiblen Daten können über die Plattform oder die App erhoben werden?
 - d. Befinden sich die Server, über die der Datenaustausch mit App oder Plattform läuft, in Österreich?
 - i. Wenn nein: Weshalb nicht?
 - ii. Wenn nein: Wo befinden sie sich?

13. Welche Sicherheitsmechanismen sind etwa bei Verlust oder Diebstahl des Handys vorgesehen?
- a. Gibt es eine durchgehend (=24/7) erreichbare Notfallnummer?
 - i. Wenn nein: Weshalb nicht?
 - b. Gibt es eine rasche Möglichkeit, den Zugang über das verlorene/gestohlene Handy zu sperren?
14. Wer trat als Veranstalter der Präsentation des digitalen Amtes am Rande der Plenarsitzung am 27.3. auf?
- a. Wurde diese Veranstaltung allein vom BMDW organisiert?
 - i. Wenn nein: Wer organisierte diese Veranstaltung mit?
 - b. Arbeiteten ausschließlich Mitarbeiter des BMDW an dieser Veranstaltung und traten dort auf?
 - i. Wenn nein: Welche nicht dem BMDW zugehörigen Mitarbeiter arbeiteten an dieser Veranstaltung oder traten dort auf?
 1. Aufgrund welcher Rechtsgrundlage arbeiteten diese an dieser Veranstaltung oder traten dort auf?
 2. Welche Kosten entstanden durch die Heranziehung ministeriumsfremder Personen?
 3. Traten dort auch Mitarbeiter des ÖVP-Parlamentsklubs auf?
 - a. Wenn ja: Aufgrund welcher Rechtsgrundlage traten diese Personen dort auf?
 - b. Verrichteten diese Personen die Arbeit daran oder das Auftreten dort innerhalb ihrer Arbeitszeit für den ÖVP-Parlamentsklub?
 - c. Welche Kosten entstanden durch die Heranziehung dieser Personen?