3339/AB
vom 14.06.2019 zu 3334/J (XXVI.GP)

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

bmdw.gv.at

Mag. Elisabeth Udolf-Strobl
Bundesministerin für Digitalisierung und Wirtschaftsstandort

elisabeth.udolf-strobl@oesterreich.gv.at
Stubenring 1, 1010 Wien

Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: BMDW-10.101/0084-Präs/4a/2019

Ihr Zeichen: BKA - PDion (PDion)3334/J-NR/2019

In Beantwortung der schriftlichen parlamentarischen Anfrage Nr. 3334/J betreffend "Bundestrojaner im "Digitalen Amt"?", welche die Abgeordneten Univ.-Prof. Dr. Alfred J. Noll, Kolleginnen und Kollegen am 16. April 2019 an meine Amtsvorgängerin richteten, stelle ich fest:

Antwort zu Punkt 1 der 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?*

Es wurden "bei der Programmierung der App" keine "Sicherheitslücken offen gelassen". Es wurden und werden vielmehr sämtliche gesetzlichen Bestimmungen eingehalten. Da die Plattform oesterreich.gv.at zugleich auch die Handy-Signatur bzw. Bürgerkarte abbildet, ist gemäß Datenschutz-Grundverordnung der Einfluss Dritter auf jeden Fall auszuschließen. Dies wurde durch die unabhängige Bestätigungsstelle (in diesem Fall durch den unabhängigen Verein A-SIT) entsprechend geprüft.

Antwort zu Punkt 2 der Anfrage:

2. *Weshalb wurde diese die App nicht als Open-Source-Software erstellt?*

Bei der Entwicklung der Plattform oesterreich.gv.at wurde eine Reihe von Open Source Software Modulen genutzt. Die Plattform ist Grundlage für die Integration von anderen Verfahren, Apps etc. und soll in der Folge auch den elektronischen Identitätsnachweis neu abbilden. Durch diese Vernetzung und Integrationsfähigkeit können nicht alle Teile als Open Source bereitgestellt werden, da die zu integrierenden Teile in der Verantwortung anderer Stellen sind.

Antwort zu Punkt 3 der Anfrage:

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?

Nein.

   d. Wenn nein: Würden Sie uns darüber informieren, wenn dem so wäre?

Ja, wenn die entsprechenden Bestimmungen in den Materiengesetzen dies zulassen.

Antwort zu Punkt 4 der Anfrage:

4. Ist in Zukunft geplant, die App "digitales Amt" als Einfallstor für Schadsoftware iSd "Bundestrojaners" heranzuziehen?
   a. Wenn ja: Inwiefern?

Nein.

   b. Wenn nein: Würden Sie uns darüber informieren, wenn dem so wäre?

Ja, wenn die entsprechenden Bestimmungen in den Materiengesetzen dies zulassen.

Antwort zu Punkt 5 der Anfrage:

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?*

Die Entwicklung der Plattform wurde vom Bundesrechenzentrum in Zusammenarbeit mit Subauftragnehmern umgesetzt. Mit dem Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz erfolgte eine technische Abstimmung zur Abrufbarkeit von Justiz-Services.

Antwort zu Punkt 6 der Anfrage:

6. Gab es im Zuge der Erstellung der Plattform oder der App eine Kooperation mit anderen Ministerien?
   a. Wenn ja: Mit welchen?

Kooperationen haben für die angebotenen Verfahren, die seitens der inhaltlich zuständigen Ressorts zu verantworten sind, stattgefunden.

Solche Abstimmungen gab es konkret mit dem Bundeskanzleramt betreffend Bundes-Content-Management-System und einheitlichem Design. Für einzelne Services wie etwa Wahlkartenbestellung, Meldung des Wohnsitzes und Babypoint stellt das Bundesministerium für Inneres Schnittstellen zu zentralen Registern wie dem Zentralen Melderegister und dem Zentralen Personenstandsregister zur Verfügung.

Für die Anbindung weiterer digitaler Serviceangebote oder die Nutzung der Chatbot Plattform sollen größtmögliche Synergien erzielt werden. Mit der Integration der eID-NEU und weiterer Verfahren werden auch künftig verantwortliche Ressorts oder andere Behörden einzubinden sein, da die Schnittstellen dort umzusetzen sind.

Antwort zu Punkt 7 der Anfrage:

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?
      iii. Wenn nein: Weshalb nicht?

iv. Wenn nein: Weshalb nicht?

Nach den Vorgaben der EU- Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) bzw. der DSGVO ist ein Vorgehen im Sinne von "Security by Design" bzw. "Datenschutz by Design" wichtig. In diesem Sinne wurden Experten von A-SITGmbH und EGIZ (E-Government Innovationszentrum), beide aus Graz, nicht nur zur Begutachtung im Sinne der Fragestellung, sondern auch zur Erstellung von Konzepten, Mustercode bzw. Codeteilen herangezogen.

Antwort zu Punkt 8 der Anfrage:

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

Ja, es wurden sowohl interne Experten als auch Experten im Bereich der für die Verfahren zuständigen Stellen konsultiert.

Antwort zu Punkt 9 der Anfrage:

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 Websiten, Magazinen uä)?

Die budgetäre Bedeckung erfolgte unter Detailbudget 40.05.01 Digitalisierung.

Die externen Kosten für die Plattformentwicklung betrugen bis zum Go Live € 5,8 Mio. Diese Kosten gliedern sich in Behördenwege inklusive aller Schnittstellen (€ 3 Mio.), Help-Migration inklusive mobil first und Infrastrukturanpassungen (€ 1,2 Mio.), eID und sichere Infrastruktur (€ 1,3 Mio.) und Bürgerbeteiligung und Usability (€ 0,3 Mio.).

Die Information über Plattform und App erfolgte in Printmedien (Biber, Bundesländerinnen Magazine, Falter, Forbes, Die Furche, Haber Avrupa, Heute, Kosmo, Kronen Zeitung, Kurier, Niederösterreichische Nachrichten, Oberösterreichische Nachrichten, Oberösterreichisches Volksblatt, Österreich, Die Presse, Profil, Regionalmedien Austria, Salzburger Nachrichten, Stadtzeitung Klagenfurt, Der Standard, Terra Mater, Trend, Tiroler Nachrichten, Wienerin,

Woman) sowie online (derstandard.at, diepresse.com, facebook.com, heute.at, Instagram, kleinezeitung.at, krone.at, kurier.at, meinbezirk.at, nachrichten.at, oe24.at, orf.at, Seven One Media Netzwerk, tt.com). Die Kosten dafür betrugen insgesamt € 1,583.994,78.

Antwort zu Punkt 10 der Anfrage:

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?

Die Umsetzung des Projekts erfolgte durch das Bundesrechenzentrum, da der Betrieb der Plattform und der notwendigen Komponenten im Bundesrechenzentrum abgewickelt wird. Da help.gv.at bereits vom Bundesrechenzentrum betrieben und komplett nach oesterreich.gv.at migriert wurde, wurde die Plattform auf dieser Basis weiter- bzw. teilweise neu entwickelt. Das Bundesrechenzentrum hat dazu Teile der Umsetzung durch eigene Ressourcen abgedeckt und jene Teile, die nicht intern abgedeckt werden konnten, bei externen Experten von Subauftragnehmern nach erfolgter EU-weiter Ausschreibung beauftragt.

Antwort zu Punkt 11 der Anfrage:

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?

Mobile Geräte sind in deutlich anderer Weise Sicherheitsrisiken ausgesetzt als Computer mit Browsern. Einerseits existiert die "schützende Browserumgebung" auf mobilen Geräten nicht in der gleichen Weise, andererseits kann man bei mobilen Geräten nicht mit einer Session mit kurzer Ablaufzeit arbeiten. Daher sind andere Konzepte, wie der Einsatz eines "Secure Element" des mobilen Gerätes, sinnvoll. Ob dieses mit Face, Touch etc. ausgelöst wird, ist dabei sekundär, da diese Informationen/Daten im Gerät verbleiben und niemals über das Netz weitergeleitet werden.

Wesentlich dabei ist, dass das Auslösen des Vorganges nicht durch das Beobachten eines vorhergehenden Vorganges bzw. durch eine andere App möglich ist und immer auch die tatsächliche Willensäußerung des Geräteinhabers erfordert. Damit ist das weitere Single Sign On für alle im E-Government und auch in der privaten Wirtschaft vorhandenen Sicherheitsstufen möglich.

Die Sicherheitsmaßnahmen sind insoweit vereinheitlicht, als für jene Applikationen, die entsprechende Sicherheitsstufen fordern, auch in der Browser-Umgebung des Computers Zweifaktor-Systeme gefordert sind. Die Verwendung der bereichsspezifischen Personenkennung ist dabei ein zentrales Element.

Antwort zu Punkt 12 der Anfrage:

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?

Betreffend Identifzierung und Authentifizierung baut die Plattform oesterreich.gv.at zentral auf der bereichsspezifischen Personenkennung auf. Damit besteht keine Notwendigkeit, weitere Informationen in Datenbanken evident zu halten, da der Zugriff auch im Sinne der Komforterhöhung durch die dahinterliegenden Services auf die authentischen Daten der Services und Register und damit nach gesetzlich klar vorgegebenen Regeln DSGVO-konform ausgelegt ist und in der Verantwortung des jeweiligen Betreibers liegt.

Wie bereits festgehalten, sind die mittels Face oder Touch übertragenen Daten ausschließlich in der Kommunikation zum Secure-Element am Gerät lokal und nicht einmal auf der Plattform selbst vorhanden, sondern nur dem System des Mobilen Gerätes zugänglich. Dies ist eine wesentliche Sicherheitsvoraussetzung, um Handysignatur bzw. später eID-Neu überhaupt einbinden zu können. Alte Geräte (bis Android Version 6), die dagegen verstoßen und eine Softwareumsetzung im Handy erlauben könnten, sind von der Verwendung der Plattform ausgeschlossen.

Betreffend Online-Services und Benutzerprofil werden prinzipiell nur Daten auf Basis der Zustimmung durch den Benutzer bzw. gesetzlicher Bestimmungen angezeigt und gespeichert. Sämtliche Daten werden ausschließlich in geschützten Bereichen auf Servern in Österreich gespeichert und nicht in der Plattform selbst. Auf die allgemeine Datenschutzerklärung https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html ist in diesem Zusammenhang zu verweisen. Bei Bedarf existiert noch eine zusätzliche Datenschutzerklärung pro Online-Service, etwa beim Babypoint.

Antwort zu Punkt 13 der Anfrage:

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?

Der Zugang über ein verlorenes bzw. gestohlenes Handy würde zusätzlich das Wissen um das Passwort der eID und das Auslösen des Secure Element erfordern. Damit ist ein Missbrauch de facto ausgeschlossen.

Zusätzlich können über den Widerrufsdienst des Vertrauensdiensteanbieters (VDA) die Bindung und die Signatur mit sofortiger Wirkung und jederzeit aufgehoben werden. Zusätzlich zur Sperre, wie diese bei kartengebundenen Signaturen stattfindet, kann danach auch nicht durch Verwendung eines falschen Datums und einer falschen Uhrzeit ein vermeintlich richtig signiertes Dokument erzeugt werden, da mit dem Widerruf der Schlüssel im Hardware Security Module des VDA gelöscht wird und damit eine weitere Verwendung gänzlich ausgeschlossen ist. Alternativ könnte ein Benutzer auch ein Login mit falschem Passwort wiederholt auslösen und damit den Schlüssel sperren. Da auch dieses Passwort in keiner Datenbank (auch nicht beim VDA) existiert und ein Rücksetzen nicht vorgesehen ist, stellt dies ebenfalls einen wirksamen Schutz dar.

Antwort zu Punkt 14 der Anfrage:

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?

Die Veranstaltung wurde alleine von meinem Ressort organisiert. Anwesend war ein Mitarbeiter der A-Trust, da ein Hauptzweck der Veranstaltung auch die Freischaltung der Handysignatur war. Die Handysignatur ist ein Produkt der A-Trust, weshalb deren Mitarbeiter befugt sind, Freischaltungen der Handysignatur durchzuführen. Meinem Ressort sind für die Mitarbeit der A-Trust keine Kosten entstanden. Mitarbeiter des ÖVP-Parlamentsklubs haben nicht an der Veranstaltung mitgewirkt.

Wien, am 14. Juni 2019

Mag. Elisabeth Udolf-Strobl

Elektronisch gefertigt

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR DIGITALISIERUNG UND WIRTSCHAFTSSTANDORT
@ AMTSSIGNATUR

Unterzeichner	Bundesministerium für Digitalisierung und Wirtschaftsstandort
Datum/Zeit	2019-06-14T09:06:57+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.	1237897311
Hinweis	Dieses Dokument wurde amtssigniert.
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/. Die Bildmarke und Hinweise zur Verifikation eines Papierausdrucks sind auf https://www.bmdw.gv.at/amtssignatur oder http://www.help.gv.at/ veröffentlicht.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2019-06-14T09:10:49+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.	