Projekt Datensicherheit von Wahlkampf-Apps

Ergebnisbericht „Datensicherheit und Datenschutz von Wahlkampf-Apps“

Autor: Prof. Dr. Dirk Pawlaszczyk
Fakultät Computer- und Biowissenschaften
Hochschule Mittweida, Technikumplatz 17, 09644 Mittweida

Ein gemeinsames Projekt des Mitteldeutschen Rundfunks (MDR) und der Hochschule Mittweida

Bearbeitungsstand: 14.08.2019

Projekt Datensicherheit von Wahlkampf-Apps

Einleitung

Der vorliegende Bericht fasst die Ergebnisse eines im Auftrag mit dem MDR durchgeführten Projektes zusammen. Es sollte die Frage geklärt werden, inwieweit Anforderungen der Datensicherheit und des Datenschutzes bei den Wahlkampf-Apps verschiedener Parteien Berücksichtigung finden. Hierfür wurden insgesamt 3 Apps von den Parteien CDU, SPD, die Grünen untersucht.

Spätestens seit den Bundestagswahlen im Jahr 2017 greifen die Parteien in Deutschland nicht nur auf die Hilfe sozialer Netzwerke und das Internet zurück. Vielmehr setzen viele Parteien auf eine gezielte Ansprache der Wähler an der Haustür. Speziell für diesen Tür-zu-Tür-Wahlkampf stellen einige Parteien mittlerweile spezielle Wahlkampf-Apps zur Verfügung. Im digitalen Zeitalter hat der direkte Kontakt zwischen Kandidat und Wähler einen ganz neuen Stellenwert. Unterstützt wird dieses Wahlkampfinstruments durch den Einsatz digitaler Technik, mit dem Ziel, die Effizienz des Tür-zu-Tür-Wahlkampfes zu verbessern. Speziell diese Funktion wurde im Rahmen dieser Studie näher betrachtet und unter Datenschutzaspekten analysiert.

Projekt Datensicherheit von Wahlkampf-Apps

Versuchsaufbau und Testumgebung

Für den Test der Apps wurde zunächst eine Untersuchungsumgebung aufgesetzt. Alle Apps wurden auf verschiedenen Smartphone-modellen und in einer virtualisierten Umgebung installiert und getestet. Als Virtualisierungsumgebung wurde VirtualBox in der Version 6 der Firma Oracle verwendet. Die Apps wurden unter Android in der 8.1.0 installiert und untersucht.

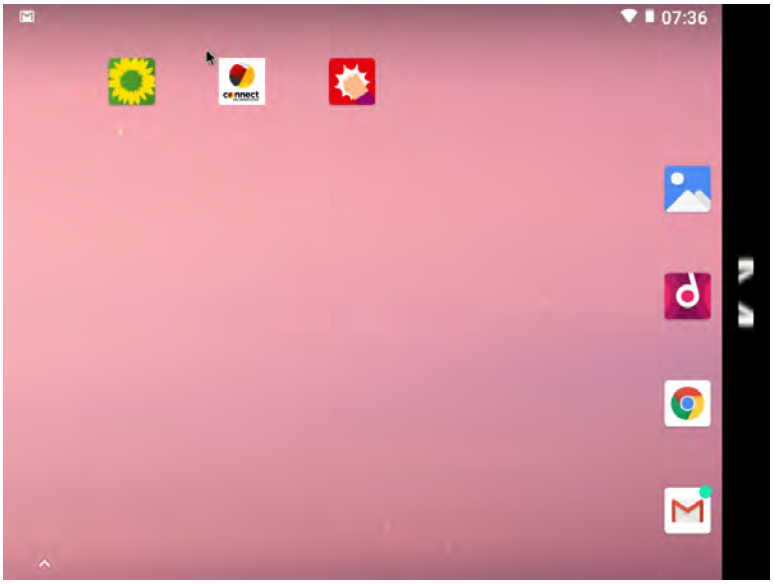

Abb. Bildschirmfoto der Virtualisierungsumgebung mit den drei getesteten Apps

Im Rahmen der Untersuchung wurden insbesondere die folgenden Punkte näher beleuchtet:

- Berechtigungen, die zum Ausführen der jeweiligen App benötigt werden
- Datenschutzbestimmungen (Inhalt, Vollständigkeit)
- Angebotene Funktionalitäten
- Verbindungsaufbau zu Servern (Welche IP-Adressen? Verschlüsselung vorhanden?)
- Konfigurationseinstellungen (Wie geschützt?)
- Lokale Log-Dateien (falls vorhanden)

Zur Untersuchung der Konfigurationsdateien wurde die virtuelle Festplatte in der Analyseumgebung als lokales Laufwerk per Mountpoint[1] eingebunden. Anschließend wurden die Verzeichnisse der jeweiligen App auf für die Ausgangsfrage hin relevante Artefakte näher analysiert.

[1] Als *Mountpoint* bezeichnet man ein Verzeichnis im Dateisystem, das als Einhängepunkt für andere Dateisysteme benutzt wird.

Datenschutz – Ein sensibler Punkt

Gemäß der Datenschutzgrundverordnung der EU und nach Bundesdatenschutzgesetz (BDSG) sind personenbezogene Daten:

*„...alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu **Standortdaten**, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind*;" (Artikel 4 DSGVO)[2].

Besondere personenbezogene Daten umfassen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit**. Sie sind besonders schützenswert**. Die Vorschriften zur Sammlung und Verarbeitung solcher Daten sind wesentlich strenger. Solche besondere Kategorien personenbezogener Daten sind gemäß § 46 Ziffer 14 a-e BDSG-neu [3](vgl. auch Artikel 4, 9 DSGVO):

*„Daten, aus denen die rassische oder ethnische Herkunft**, politische Meinungen**, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen"*

Oft ist unklar, ob es sich mit Hilfe einer bestimmten Information auf eine oder mehrere Personen schließen lässt bzw. ob Ihnen diese zugeordnet werden kann. Im Falle einer Angabe der Straße samt Hausnummer und Ort ist das beispielsweise anzunehmen. Zwar fehlt in diesem Fall der Name. Dennoch genügen diese Angaben häufig um Personen indirekt zu identifizieren, durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen. Das Gegenteil zu beweisen ist oft zeitaufwendig und ist speziell, wenn sehr viele Datensätze zu verarbeiten sind, praktisch nur schwer durchführbar. Sobald wir in einer Straße beispielsweise ein Einfamilienhaus finden, dann ist eine Zuordnung zu einer Person oder Personenkreis möglich.

Grundsätzlich sind all jene Daten, die eindeutige Informationen enthalten können, als personenbezogen anzusehen, auch dann, wenn sie nicht selbst (und nachweislich ohne Personenbezug) generiert wurden.

Anders ausgedrückt genügt es bereits, dass eine Information in einigen Fällen dazu verwendet werden kann, um diese in Zusammenhang mit einer Person zu bringen, auch wenn dies gar nicht beabsichtigt ist. Auch weniger eindeutige Informationen können einen Personenbezug ermöglichen. Im Zusammenhang mit den untersuchten Apps ist zunächst festzustellen, dass diese unterschiedliche Arten von Daten erfassen. Dabei lassen sich grob drei Kategorien unterscheiden:

1. Informationen, die über die Benutzer der App (die Wahlkämpfer) erfasst werden,
2. Informationen, die über Wähler bzw. Wählergruppen und deren politische Einstellungen in einem bestimmten Gebiet erfasst werden, repräsentiert durch GPS-Koordinaten,
3. personenbezogene Informationen über Unterstützer der Partei, wie bei der Connect-App der CDU.

---

[2] *https://dsgvo-gesetz.de/art-4-dsgvo/*
[3] *http://www.gesetze-im-internet.de/bdsg_2018/*

Dabei folgen die Parteien offenbar dem Credo: **Sag mir, wo du wohnst, und ich sage dir, was du wählst**. Die Informationen der Kategorie 1 und 3 haben einen eindeutigen Personenbezug und werden auch von den Parteien in den untersuchten Programmen als solche eingestuft. Damit fallen diese unter die Bestimmungen der Datenschutzgrundverordnung.

Gerade bei der zweiten Datenkategorie stellt sich allerdings die Frage, ob es sich tatsächlich um personenbezogene Daten im Sinne der DSGVO handelt oder nicht vielleicht doch um reine Sachdaten.

Bei den durch die Apps erhobenen **Geodaten** in Form von GPS-Koordinaten - die sich gerade durch ihre raumbezogene Referenzinformation auszeichnen - ist es so gut wie immer möglich, diese Referenzinformation mit Koordinaten und/oder Adressen und diese wiederum mit Personen zu verknüpfen, es sei denn, sie werden anonymisiert.

Speziell in diesem Bereich herrscht schon seit Jahren eine anhaltende Diskussion über die Bestimmbarkeit dieser Daten. Mit dem Begriff **Bestimmbarkeit** ist hiermit gemeint, ob es möglich ist, einen Personenbezug für ein gegebenes Datum herzustellen oder eben nicht. Gerade bei Geodaten besteht das Problem, dass ein Personenbezug zu einer Standortangabe oder Adresse meist ohne großen Aufwand und für jedermann zugänglich über das Internet hergestellt werden kann – etwa über Google Street View. Beschreiben die Daten hingegen eine Sache, zu der nur zufällig auch natürliche Personen in Beziehung stehen, zu denen die Verarbeitung der Sachdaten aber in keinerlei Zusammenhang steht, handelt es sich um **Sachdaten**. Sofern kein bewusster personenbezogener Verarbeitungszusammenhang besteht, fallen Geodaten nicht unter die DSGVO.

Liegt ein Personenbezug vor, ist folglich die Erfassung und Verarbeitung von Geoinformationen nur mit Zustimmung der Betroffenen zulässig. Speziell mit dieser Frage beschäftigen sich auch die im Folgenden vorgestellten Untersuchungsergebnisse. Diese werden gesondert für jede Partei und deren App kurz vorgestellt und besprochen.

Die Wahlkampf-App *CDU-connect-App*

Für den Test wurde die App der CDU in der aktuellen Version 2.2.1 vom 23. Mai 2019 getestet. Laut Google Playstore wurde diese bereits mehr als 5000-mal heruntergeladen und installiert.

Funktionsumfang

Das von der CDU für Unterstützer der Partei über Playstore zur Verfügung gestellte Programm bietet, verglichen mit den anderen untersuchten Programmen, den größten Funktionsumfang. So werden u.a. die folgenden Optionen angeboten: Tür-zu-Tür, Vandalismus, Themen, Unterstützer, Bürgerfrage sowie eine Rangliste der bislang fleißigsten Wahlhelfer.

Die App wird derzeit aktiv in verschiedenen Kampagnen der CDU eingesetzt. Für den Test wurde die Kampagne „Sachsenwahl“ verwendet. Als weitere Informationen müssen Kreisverband und Wahlkreis, in welchem der Unterstützer tätig ist, angegeben werden.

Anmeldung

Zur Nutzung der App ist eine vorhergehende Registrierung erforderlich. Eine Anmeldung kann wahlweise über Facebook oder per Mail erfolgen. Es ist anzumerken, dass die Anmeldedaten dabei offenkundig nicht lokal hinterlegt werden und somit auch nicht gestohlen oder anderweitig missbraucht werden können. Die Anmeldung erfolgt über das Webportal der CDU. Auffällig ist, dass bei der Angabe des Passworts keine besonderen Sicherheitsmerkmale verlangt werden. Ein einfaches „passwort“ genügt. Eine Mindestlängenangabe, die Verwendung von Zahlen und Sonderzeichen wird offenkundig nicht verlangt.

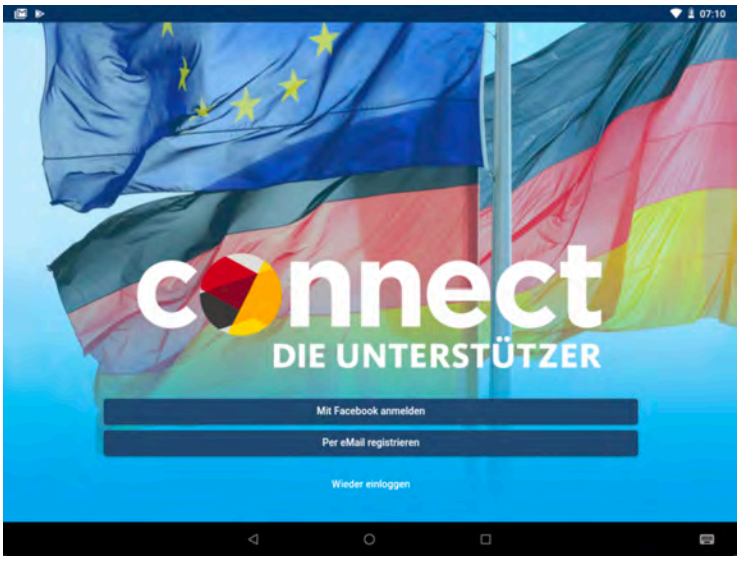

Abb. Der Startbildschirm der App mit Anmeldeoptionen

Berechtigungen

Die App benötigt die Berechtigung zur Standortbestimmung und ggf. Zugriff auf Verzeichnisse des Mobiltelefons.

Verbindungsaufbau zu Servern

Bei der Aufzeichnung des Datenverkehrs zeigt sich, dass die App fast ausschließlich mit der IP 193.219.105.84 kommuniziert. Die IP ist registriert auf die Union Betriebs GmbH, ansässig in Rheinbach, Nordrhein-Westfalen. Die Verbindung ist verschlüsselt (TLSv1.2).

87	12.621081	192.168.178.103	193.219.105.84	TCP	74	51660 → 443 [SYN]
88	12.798470	193.219.105.84	192.168.178.103	TCP	76	443 → 51660 [SYN,
89	12.798825	192.168.178.103	193.219.105.84	TCP	66	51660 → 443 [ACK]
90	12.799155	192.168.178.103	193.219.105.84	TLSv1.2	583	Client Hello
91	12.841153	193.219.105.84	192.168.178.103	TLSv1.2	207	Server Hello, Chan
92	12.841523	192.168.178.103	193.219.105.84	TCP	66	51660 → 443 [ACK]
93	12.841837	192.168.178.103	193.219.105.84	TLSv1.2	117	Change Cipher Spec
94	12.842081	192.168.178.103	193.219.105.84	TCP	1506	51660 → 443 [ACK]
95	12.842081	192.168.178.103	193.219.105.84	TLSv1.2	920	Application Data
96	12.842272	192.168.178.103	193.219.105.84	TLSv1.2	389	Application Data
99	12.893057	193.219.105.84	192.168.178.103	TCP	68	443 → 51660 [ACK]
100	12.893060	193.219.105.84	192.168.178.103	TCP	68	443 → 51660 [ACK]
103	13.029704	193.219.105.84	192.168.178.103	TCP	1506	443 → 51660 [ACK]
104	13.029708	193.219.105.84	192.168.178.103	TCP	1506	443 → 51660 [ACK]
105	13.029818	193.219.105.84	192.168.178.103	TCP	1506	443 → 51660 [ACK]
106	13.029820	193.219.105.84	192.168.178.103	TLSv1.2	799	Application Data
107	13.030232	192.168.178.103	193.219.105.84	TCP	66	51660 → 443 [ACK]

Abb. Auszug eines Datenmitschnitts der Connect-App mit Wireshark

Untersuchung der lokalen Installationsverzeichnisse

Eine Untersuchung der lokalen Anwendungsverzeichnisse ergab keine besonderen Auffälligkeiten.

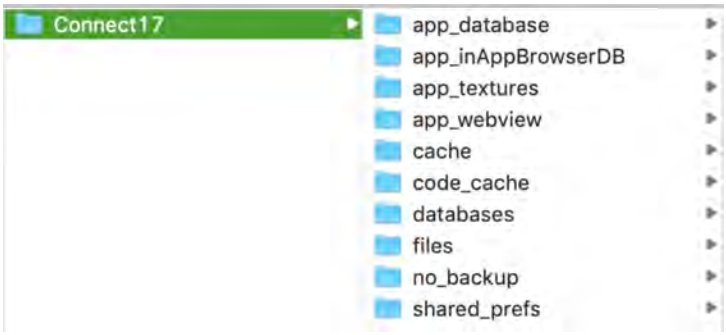

Abb. Lokale Verzeichnisstruktur der App (auf dem Smartphone)

Offenbar werden praktisch alle Daten direkt an den Server der CDU übermittelt. Eine Zwischenspeicherung auf dem Gerät selbst erfolgt scheinbar nicht. Zumindest konnten keine Datenspuren oder Anhaltspunkte dafür gefunden werden. Lediglich eine Reihe von Cookies wird auf dem Gerät hinterlegt in der Datei:

`data/data/Connect17/app_webview/Cookies`

Hier werden unter anderem die SessionsIDs für die Verbindung mit dem CDU-Server, die nach erfolgreicher Anmeldung an der App automatisch erzeugt werden, gespeichert.

	creation_utc	host_key	name	value	path
	Filtern	Filtern	Filtern	Filtern	Filtern
1	13209917352520171	cdu.kampagnen-dialog.de	XSRF-TOKEN	eyJpdiI6IjhyOHh4TkQyM1AzeXRGaW41c0hHSHc9PSIsInZhbHVlIjoiYnFKQWZvTmUyW...	/
2	13209917352520209	cdu.kampagnen-dialog.de	laravel_session	eyJpdiI6Im0ySlwvb2N3V1BqY25mXC94QUw2VVZoUT09IiwidmFsdWUiOiJCWWxlUW5...	/
3	13209973346446817	www.cdu.de	has_js	1	/
4	13209973370904237	www.cdu.de	cookie-agreed	2	/
5	13209973370905124	www.cdu.de	ubg_privacy_piwik	false	/

Abb. Auszug aus der Cookie-Datenbank der App.

Datenschutz

Die Datenschutzbestimmungen sind sehr umfangreich und detailliert formuliert. Personenbezogene Daten werden an verschiedenen Stellen der App erhoben (beispielsweise bei der App-Funktion Unterstützer). Der Nutzer muss aber in jedem Fall durch Unterschrift auf dem Gerät einer Verarbeitung seiner Daten ausdrücklich zustimmen.

Die Tür-zu-Tür Wahlkampffunktion der App bestimmt auf Wunsch automatisch die Position. Man kann alternativ auch die Straße manuell eingeben. Es werden neben der Meinung zur CDU lediglich Straßenname, Postleitzahl und Ort der Erfassung erhoben. Statt der genauen GPS-Daten wird lediglich der Straßenname über das Formular erfasst. In diesem Sinne kann nicht von echten personenbezogenen Daten gesprochen werden.

Fazit

Die Connect-App ist in Punkto Datensicherheit und Datenschutz als gut einzustufen. Es werden keine personenbezogenen Daten auf dem Gerät gespeichert. Wo personenbezogene Daten erfasst werden, müssen die Betroffenen auch immer mit Ihrer Unterschrift der Verarbeitung bzw. Weitergabe explizit zustimmen. Einziger Kritikpunkt ist die fehlende Abfrage von Sicherheitsmerkmalen bei der Festlegung des Nutzerpassworts.

Die Wahlkampf-App SPD-TzT

Für den Test wurde die App der SPD in der aktuellen Version 1.0 vom 10. Dezember 2018 getestet. Laut Google Playstore wurde diese bereits mehr als hundertmal heruntergeladen und installiert.

Funktionsumfang

Das von der SPD über Playstore zur Verfügung gestellte Programm bietet, verglichen mit den der Connect-App der CDU, einen deutlich geringeren Funktionsumfang. So wird lediglich die Möglichkeit angeboten, den Tür-zu-Tür Wahlkampf durch einen Fragebogen zu unterstützen, um mehr über die den Wählern am Herzen liegenden Wahlthemen zu erfahren. Als zweites Feature wird die Erfassung von Vor– und Familienname und Email-Adresse über ein Kontaktformular angeboten, um Interessierte mit einem Newsletter informieren zu können.

Die App wird derzeit aktiv in verschiedenen Kampagnen der SPD eingesetzt. Für den Test wurde die Kampagne „LTW Sachsen“ ausgewählt.

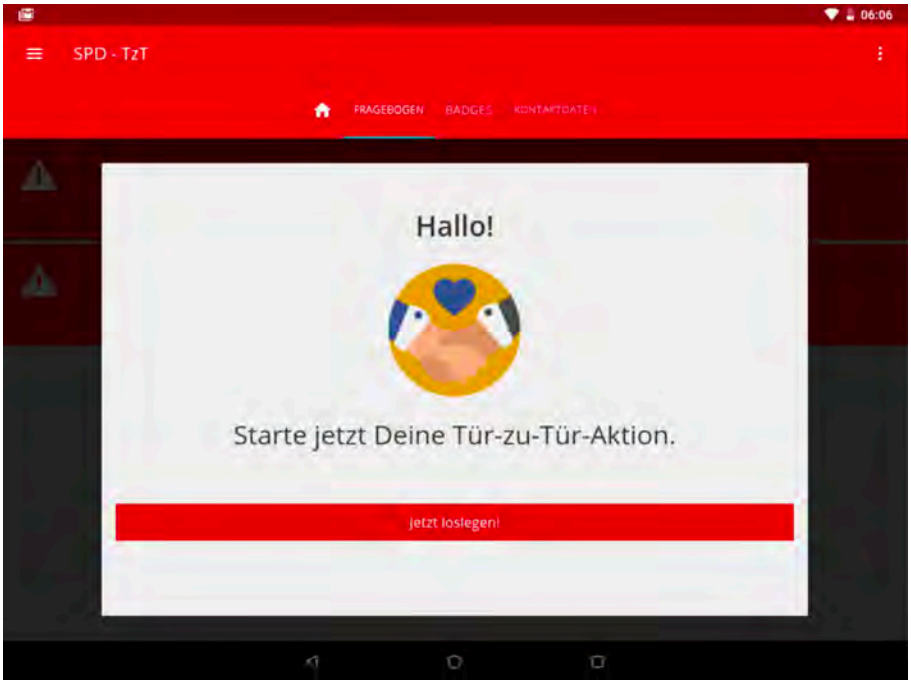

Abb.: Bildschirmaufnahme des SPD-TzT-App

Anmeldung

Zur Nutzung der App ist eine vorhergehende Registrierung erforderlich. Eine Anmeldung erfolgt per Mail. Es ist anzumerken, dass die Anmeldedaten dabei offenkundig nicht lokal hinterlegt werden und somit auch nicht gestohlen oder anderweitig missbraucht werden können. Die Anmeldung erfolgt über das Webportal der SPD. Bei der Festlegung des Passworts wird auf Sicherheitsmerkmale geachtet.

Berechtigungen

Die App benötigt die Berechtigung zur Standortbestimmung und ggf. Zugriff auf Verzeichnisse des Mobiltelefons.

Verbindungsaufbau zu Servern

Bei der Aufzeichnung des Datenverkehrs zeigt sich, dass die App fast ausschließlich mit der IP 80.82.200.232 kommuniziert. Die IP ist registriert auf die SPD. Die Verbindung ist verschlüsselt (TLSv1.2).

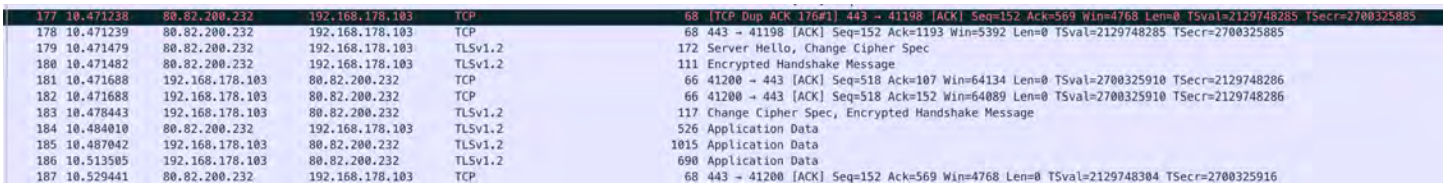

Abb. Auszug eines Datenmitschnitts der SPD-TzT-App mit Wireshark

Speicherort: `data/data/SPT-TzT/app_webview/Cookies`

Untersuchung der lokalen Installationsverzeichnisse

Eine Untersuchung der lokalen Anwendungsverzeichnisse ergab keine besonderen Auffälligkeiten. Wie auch die Connect-App verwendet dieses Programm einen eingebauten Webbrowser (Webview) um die zumeist formulargestützten Eingaben durchzuführen. Anders ausgedrückt werden also lediglich einige Webseiten auf dem SPD-Portal aus der App heraus aufgerufen und mit Daten gefüllt. Eine lokale Datenhaltung durch die App selbst findet somit nicht statt bzw. es finden sich keine Hinweise darauf.

Ebenso wie bei der Connect-App der CDU werden keine relevanten Daten auf dem Gerät selbst gespeichert, und stattdessen immer direkt an den Server weitergeleitet. Die App dient wiederum der reinen Datenerfassung. Lediglich einige Cookies werden auf dem Smartphone abgelegt.

Datenschutz

Die Datenschutzbestimmungen sind ausreichend und klar formuliert. Personenbezogene Daten werden bei der Funktion „Kontakt-daten für den Newsletter“ abgefragt. Im Unterschied zur Connect-App wird in diesem Fall aber auf eine schriftliche Zustimmung des Betroffenen verzichtet.

Allein das handschriftliche Notieren von Kontaktdaten stellt noch keine Verarbeitung von personenbezogenen Daten i.S.d. DSGVO dar. In diesem Fall würde das Datenschutzrecht nicht greifen. Über die bereitgestellte Funktion der SPA-TzT-App werden allerdings die Kontaktdaten elektronisch erfasst, um an die Betroffenen einen Newsletter zu versenden.

Da auf dem Wahlkampfstand die Besucher regelmäßig selbst ihre Daten an die Partei weitergeben, kann hier grundsätzlich von einer (auch mündlich oder durch konkludentes Handeln möglichen) Einwilligung zur elektronischen Erfassung der Daten ausgegangen werden. Der Nachweis einer nicht schriftlich abgegebenen Einwilligung ist jedoch schwierig. In der Regel kann sich die Partei aber auch auf die Interessenabwägung als Erlaubnisnorm berufen.

Die Tür-zu-Tür Wahlkampffunktion der App bestimmt auf Wunsch automatisch die Position. Man kann alternativ auch die Straße – genauer gesagt den Straßenabschnitt - manuell eingeben (Beispiele: 218-2R8 218-2UB 217-P7A). Es wird insbesondere die Meinung zu bestimmten Wahlkampfthemen abgefragt. Darüber hinaus werden Straßenname, Postleitzahl und Ort bei der Erfassung des Datensatzes erhoben. In diesem Sinne kann nicht von echten personenbezogenen Daten gesprochen werden. Eine Anonymisierung findet bereits im Programm über die erwähnten Straßenabschnitte statt. GPS-Daten werden offenkundig nicht erhoben.

Fazit

Die SPT-TzT-App ist in Punkto Datensicherheit und Datenschutz als gut einzustufen.

Die Wahlkampf-App der Grünen

Für den Test wurde die App der Partei die Grünen in der Version 1.1.1 vom 17. Mai 2019 getestet. Laut Google Playstore wurde diese bereits mehr als 1000mal heruntergeladen und installiert. Auch lassen sich keinerlei Hinweise darauf finden, dass die Software sich noch im Beta-Stadium befindet, weder im Playstore noch innerhalb der Anwendung. Offenbar handelt es sich also nicht um eine bloße Testversion.

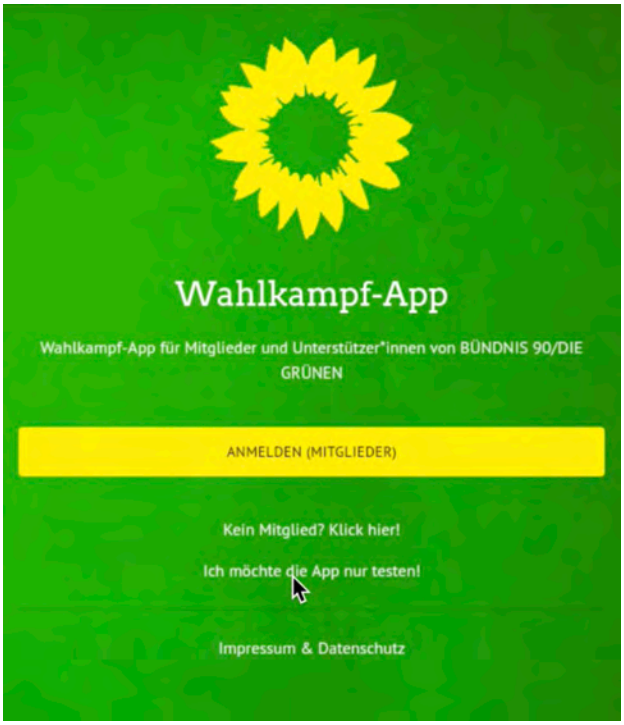

Abb. Startbildschirm der Grünen Wahlkampf-App

Anmeldung

Für die Analyse wurde die App in einem speziellen Test-Modus ausgeführt und getestet. Eine Überprüfung der Anmeldung war leider nicht möglich, da unsere Anfrage bei den Grünen leider bis dato unbeantwortet geblieben ist.

Funktionsumfang

Für die Funktion des Tür-zu-Tür Wahlkampfs ist es erforderlich, zunächst eine sogenannte Session (zu deutsch Sitzung) anzulegen. Unter der Sitzung werden anschließend alle Informationen, die der Wahlkämpfer sammelt, zusammengefasst. Nach dem die App gestartet wurde, kann man verschiedene Funktionen anwählen. Im Rahmen der weiteren Untersuchungen wurde speziell die Tür-zu-Tür Wahlkampf – Funktion getestet.

Berechtigungen

Die App benötigt die Berechtigung zur Standortbestimmung und ggf. Zugriff auf einzelne Verzeichnisse des Mobiltelefons.

Untersuchung der lokalen Installationsverzeichnisse

Im Gegensatz zu den beiden anderen getesteten Apps verfolgt das Programm der Grünen eine grundsätzlich andere Philosophie bei der Speicherung der Dateninhalte. So werden die Daten nach der Erfassung nicht direkt auf den Server übertragen. Vielmehr erfolgt eine lokale Zwischenspeicherung der im Tür-zu-Tür-Wahlkampf erfassten Datensätze. Erst die endgültige Freigabe durch den Nutzer bewirkt eine Übertragung auf den Server. In der Zwischenzeit können die erfassten Daten jederzeit nachbearbeitet werden. Folglich lassen sich auch Datenspuren der gesammelten Daten auf dem mobilen Gerät finden. Die Datensätze sind in einer Datenbank auf dem internen Speicher des Mobiltelefons abgelegt.

Lage der Datenbank im Dateisystem:

```
data/data/de.gruene.wkapp/databases/gruene_wk.db
```

Datenschutz

Die Datenschutzbestimmungen sind klar formuliert. Unter dem Aspekt des Datenschutzes wurde weiterhin untersucht, welche Informationen von den Wahlkämpfern über die App erfasst, gespeichert und zur Weiterverarbeitung an den Server versendet werden. Die App speichert zwar keine Namen, die eindeutig personenbezogene Daten darstellen würden. Davon abgesehen werden allerdings Angaben über Straße, Hausnummer, Geo-Positionsdaten sowie die Einstellung des/der Befragten zur Partei über ein Formular erfasst und anschließend gespeichert.

Tabelle: tuerZuTuerDB — Neue Zeile

	timestamp	lat	lon	wk_nr	user	street	housenumber	zipcode	city	date	time	opened	reaction	electprobability
1	1565411725889	52.51811425184304	13.379432412330063	null	99999999	B2	114	10117	Berlin	10.08.2019	06:35	true	4	2
2	1565411757587	52.51811425184304	13.379432412330063	null	99999999	B2	114	10117	Berlin	10.08.2019	06:35	true	3	2
3	1565411984219	52.517604890634246	13.377299741841854	null	99999999	B2	25	10117	Berlin	10.08.2019	06:39	true	3	2

Abb. Ansicht der Tabelle *tuerZuTuerDB* aus der Datenbank der App

Nachweislich werden die Daten dabei lokal auf dem Gerät zwischengespeichert. Auch wenn die Daten möglicherweise auf dem Server später anonymisiert werden, so ist diese Praxis nicht datenschutzkonform. Nach BDSG und DSVGO ist bereits die Erhebung personenbezogener Daten nur zulässig, wenn der Betroffene eingewilligt hat. Wenn wir davon ausgehen, dass es sich bei den Datensätzen (Geo-Position, Straße, Hausnummer) um personenbezogene Daten handelt, dann ist auch die Speicherung - egal aus welchem Grund - zustimmungspflichtig. Es gilt zudem immer der Grundsatz der **Datensparsamkeit**. Selbst dann, wenn für eine statistische Auswertung letztlich nur die Straße verwendet wird, dürften andere Informationen wie Hausnummer oder Positionsdaten nicht mit erfasst werden. Nach eigener Aussage der Grünen werden die erfassten Daten auf dem Server unter der gleichen Adresse zusammengeführt. Diese Aussage wird durch ein Screencast-Video zur Bedienung der App bestätigt.[4] Die Angaben werden offenbar dazu verwendet, eine Art „Wahlkampf-Atlas“ zu erstellen. So kann jeder angemeldete Nutzer der App sofort sehen, an welcher Hausnummer andere Wahlkämpfer bereits geklingelt haben.

[4] *Youtube-Video der Grünen: https://www.youtube.com/watch?v=HLqc6kZkfkA*

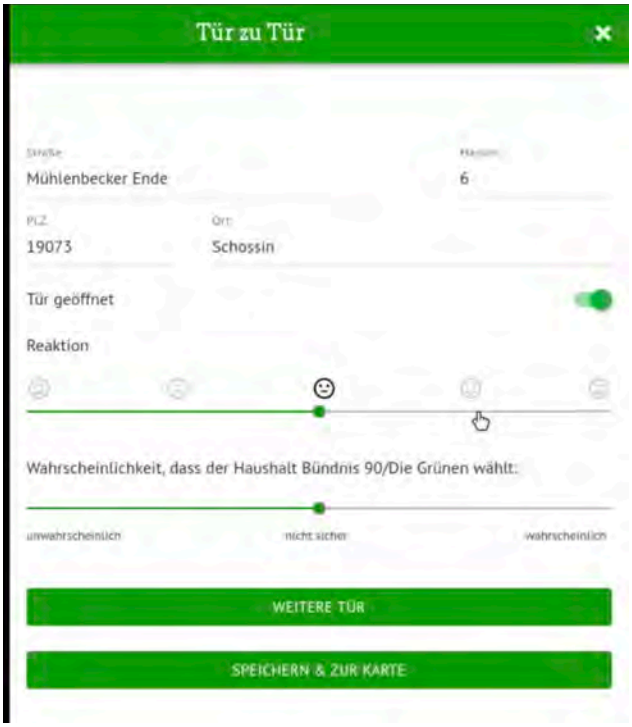

Abb. Erfassungsmaske über die Reaktion von Bürgern und deren wahrscheinlicher Wahlbereitschaft für die Grünen

Fazit

Die Wahlkampf-App der Grünen ist in der getesteten Version in Punkto Datensicherheit und Datenschutz leider nicht in allen Belangen datenschutzkonform. Speziell die Tür-zur-Tür-Funktion erfasst Informationen über die politische Einstellung von Personen bzw. die Affinität zur Partei. Dabei werden zwar keine Namen aufgezeichnet. Für jeden Datensatz werden allerdings die GPS-Positionsdaten gespeichert. Gerade bei Geodaten besteht das Problem, dass ein Personenbezug zu einer georeferenzierten Ortsangabe oder Adresse meist ohne großen Aufwand hergestellt werden. Somit können auch über die App erfasste Daten durch die Positionsangabe im ungünstigen Fall direkt einer natürlichen Person bzw. einem Personenkreis zugeordnet werden. Aus dieser Überlegung heraus sind die erfassten Daten nicht als reine Sachendaten sondern **personenbezogene Daten** einzustufen. Im Vergleich dazu setzen die Apps von SPD und CDU auf eine Anonymisierung der Angaben. Indem lediglich Straßenname bzw. Straßenabschnitte erfasst werden, soll eine direkte Zuordnung verhindert werden. Außerdem problematisch ist die lokale Zwischenspeicherung der Daten. Denn gerade für die Speicherung personenbezogener Daten bestehen besonders hohe Anforderungen an die Datensicherheit.

Ohne die ausdrückliche Zustimmung der Betroffenen ist eine solche Form der Datenerhebung aus Sicht des Datenschutzes grundsätzlich als bedenklich zu bezeichnen.