DOXXING - Gute Vorsätze für 2019: Ich werde meine Daten-Privatsphäre besser schützen!

Dienstag, 08 Januar 2019

https://www.datenschutz.de/doxxing-gute-vorsaetze-fuer-2019-ich-werde-meine-daten-privatsphaere-besser-schuetzen/

Wie? Der TLfDI sagt es Ihnen, wie es geht:

Pressemitteilung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit vom 07.01.2019

Die Veröffentlichung von persönlichen und zum Teil auch sehr vertraulichen Daten von Politikern, Prominenten und Journalisten im Internet ist in aller Munde. Dabei ist noch nicht ganz klar, auf welchen Wegen die Daten erlangt wurden. Soziale Netzwerke scheinen jedoch eine Rolle zu spielen. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nimmt die Vorfälle zum Anlass, um auf seine Broschüre „Digitale Selbstverteidigung“ hinzuweisen. „Selbstschutz setzt allerdings aktives Handeln voraus – wenn Sie es nicht tun, macht es keiner“, so Dr. Lutz Hasse.

Hier werden unter anderem die folgenden Maßnahmen empfohlen (siehe: https://www.tlfdi.de/mam/tlfdi/wir-ueber-uns/digitale_selbstverteidigung_bro-schure_3.web.pdf):

– Der Zugang zu Online-Accounts sollte durch ein starkes Passwort geschützt sein (min. 8 Zeichen, keine Wörter, Groß- & Kleinbuschstaben, Ziffern, Sonderzeichen). Zudem sollte für jeden Account ein anderes Passwort verwendet werden. Wenn möglich, sollte zusätzlich zum Passwort eine Zwei-Faktor-Authentisierung genutzt werden.

– E-Mail-Anhänge unbedingt nur dann öffnen, wenn Absender, Betreff und E-Mail-Text plausibel sind!

– Bankverbindungen, Passwörter usw. sind sehr vertrauliche Daten und sollten nicht unbedacht verwendet werden. Man sollte bei Verwendung vor allen Dingen darauf achten, dass eine Verschlüsselung der Webseite (z.B. bei Online-Shopping, Online-Banking) genutzt wird. Man erkennt dies an der Verwendung von https:// im Internetlink.

– Die genutzten Computer und Mobilgeräte sollten mit regelmäßigen Updates der Software und der Betriebssysteme unterzogen werden.

– Die genutzten Computer und Mobilgeräte sollten mit aktuellen Antiviren-Programmen ausgestattet sein, die ebenfalls regelmäßig geupdatet werden müssen.

– In sozialen Netzwerken sollten Sie ebenfalls keine vertraulichen Daten (wie Familienfotos, Kinderfotos, Kontonummern, Ausweis-Scans) an Personen oder Chatgruppen versenden, denen Sie nicht aus persönlichen (Echtwelt-)Kontakten vertrauen können.

– Nützlich sind Messenger, die zwischen Nachrichtensender und –empfänger heute schon Textdaten, Sprachnachrichten, Videochats, Bilder und Dateianhänge verschlüsseln. Auf dem Gerät werden die Daten allerdings nur noch mit der Systemverschlüsselung gesichert – wer also das Smartphone „knackt“, hat auch auf diese Daten Zugriff. Das Smartphone sollte also auch mit PIN bzw. Passwort gesichert werden. Außerdem sammeln Messenger-Anbieter möglicher Weise auch Metadaten (etwa Nutzerkennung der Gesprächsteilnehmer) oder gar Klardaten (etwa Adressbucheinträge) und diese landen evtl. auch bei Daten-Händlern. Hier sollte man also auch vorsichtig sein und kritisch hinterfragen, welchen Messenger man nutzt und ob man nicht besser einen sichereren Messenger vorzieht, auch wenn er vielleicht nicht so anwenderfreundlich ist.

Dr. Hasse rät: „Minimieren Sie Ihre Daten im Netz – Ihre Daten werden genutzt, um Profile über Sie zu erstellen, ohne dass Sie es wissen. Und diese Profile werden wiederum genutzt, um Feststellungen oder Prognosen über Sie zu treffen. Diese müssen nicht stimmen, werden aber gleichwohl verwendet. Von wem und zu welchem Zweck
– unbekannt!“

Jedermann sollte daher den Betrieb eines Kontos in einem sozialen Netzwerk kritisch prüfen. Wer nun sein Konto sogar löschen möchte, sollte die Mühen nicht scheuen und die dortigen Hinweise zum Löschen von Accounts lesen und umsetzen.

Die Pressemitteilungen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit können hier abgerufen werden.
