A 33.1/34.1 – GeoApps und Datenschutz am eigenen Smartphone

Grundsätzlich versuche ich, dass ich nur jene Apps installiere, welche ich auf wirklich benötige, um nicht grundlos Daten an Dritte weiterzugeben. Ich habe immer Passwörter, welche Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen beinhalten, um meine Zugänge bestmöglich zu schützen. Bei manchen Seiten und Apps habe ich das Passwort gespeichert aber nur bei jenen, welche mir nicht so wichtig erscheinen. Wahrscheinlich sollte ich mich darüber näher erkundigen und auch bei scheinbar harmlosen Seiten meine Passwörter nicht speichern. Generell schreibe ich beispielsweise aber keine Passwörter in meine Notizen, wobei dies meiner Erfahrung nach viele Menschen machen. Ich logge mich bei diversen Internetseiten immer aus, um nicht die ganze Zeit mit meinem Konto angemeldet zu sein, falls ich mein Handy oder meinen Laptop verlieren sollte.

Bei meinem Iphone haben mich meine Ortungsdienste-Einstellungen positiv überrascht. Ich habe fast überall eingestellt, dass die App meinen Standort „nie“ freigeben darf. Nur bei einigen wenigen Apps, wie z. B. Garmin App (fürs Lauftracking), Easy Park (Bezahlapp für die Kurzparkzonen), Google Maps, Lieferando, ÖBB App, Instagram und Snapchat darf „beim Verwenden der App“ auf meinen Standort zurückgegriffen werden. Bei allen anderen elf Apps darf nie darauf zugegriffen werden. Nur bei zwei Apps, u. a. Whatsapp, ist eingestellt, dass diese immer auf meinen Standort zugreifen können. Dies habe ich sofort geändert. Bei meinem Laptop ist der Positionszugriff ebenfalls ausgeschaltet und keine Apps können darauf zugreifen. Im Gegensatz dazu sind der Kamera- und Mikrofonzugriff bei etlichen Apps erlaubt. Dies erfolgte wahrscheinlich dadurch, dass man beim Verwenden der App oft auf „Zustimmen“ drückt und man sich dann keine Gedanken mehr dazu macht. Man sollte also gut überlegen, bei welchen Apps ein Zugriff auf Kamera und Mikrofon notwendig ist.

Das Thema Social Media ist sehr umstritten. Ich für meinen Teil bin dabei wirklich sehr vorsichtig. Ich benutze z. B. bloß Instagram und Facebook regelmäßig. Snapchat wende ich nur sehr selten an. Meine persönlichen Einstellungen sind sehr privat. Bei allen Accounts im Social Media Bereich bin ich auf „privat“ gestellt. Das bedeutet, dass Menschen keine Infos von mir sehen können, bevor ich sie nicht als Freundin/Freund akzeptiert habe. Auch bei Snapchat kann man mir ohne „Erlaubnis“ keine Bilder schicken. Dies kann ich deshalb sagen, weil ich meine Einstellungen und meine Sichtbarkeit ständig überprüfe. Bei Facebook kann man z. B. eine Rolle als fremde*r Nutzer*in einnehmen und man sieht das eigene Profil aus Sicht einer fremden Person. Dahingehend bin ich also sehr gut geschützt. Nichtsdestotrotz sieht man immer häufiger, dass Menschen, vor allem junge Leute, öffentliche Profile haben und man einfach alles sehen kann. Dies schränkt die Privatsphäre enorm ein. Natürlich hat dies auch mit eventuellen Mobbingattacken zu tun, weil jede Person weltweit anonym Kommentare hinterlassen kann. Auch bei Snapchat kommt es extrem oft vor, dass Bekannte von mir sehr abartige Bilder bekommen, da man öffentlichen Personen auch alles schicken kann. In solchen Fällen verstehe ich den Sinn nicht. Ich weiß aber trotzdem nicht, warum diese Bekannten die Einstellungen nicht ändern wollen. Dies muss jedoch jede Person individuell für sich entscheiden. Es muss auch jede*r für sich entscheiden, inwiefern sie*er sein Leben mit der öffentlichen Community teilen möchte. Gerade als zukünftige Lehrperson sehe ich mich in einer Situation, wo ich definitiv nichts durch meine digitale Identität preisgeben möchte. Kinder und Jugendliche kennen sich in der digitalen Welt schon so gut aus und wissen, wie man zu Daten kommt. Aus diesem Grund ist es umso wichtiger, sich selbst mit der Thematik auseinanderzusetzen. Man sollte in einer Weise einen guten Überblick über die eigene Situation haben. Natürlich ist es nicht möglich, alles zu überwachen und man gibt bestimmt Daten weiter, ohne es bewusst zu bemerken. Meiner Meinung nach sollte man trotzdem hin und wieder seine eigenen Daten prüfen und möglicherweise manche Einstellungen ändern.

Patricia Salzwimmer