

Das Internet verliert

Fast täglich kommen E-mails, die mich zur Preisgabe von Daten verleiten wollen. Ab und zu auch Erpressungsversuche. Das bedeutet für mich, dass ich E-mails besonders aufmerksam kontrollieren muss und auch schon Erpressungsversuche bei der Polizei angezeigt habe. All das kostet Zeit und Nerven. Auch beim Besuch von Internetseiten ist Aufmerksamkeit und Sorgfalt wichtig, um die Hoheit über die eigenen Daten nicht zu verlieren.

Wo führt das hin? Ich fürchte, dass die Benutzung des Internets immer umständlicher und immer weniger sicher wird, was die einst sympathische Idee ruinieren könnte. Der Bayerische Rundfunk hat in einem Beitrag zusammen gefasst, was man tun sollte, wenn man seine Daten nicht gefährden will. Schon in der Überschrift heißt es: „Passwort war gestern“.

Erster Schritt: Man soll einen Passwortmanager installieren, der sichere Passwörter erzeugt und speichert. Die im Browser vorhandenen seien nicht sehr sicher. Je komplexer ein Passwort, desto sicherer. Aber das ist eigentlich kein Passwort mehr, sondern eine Zeichenkette, die sich niemand mehr merken kann. Deswegen braucht man dafür einen Passwortmanager.

Zweiter Schritt: Damit man das richtig macht und keine Schwachstelle übersieht, solle man sich alle Accounts (Zugänge) aufschreiben und dann bei allen:

Dritter Schritt: Nur noch sichere Passwörter verwenden. Die kann man sich allerdings nicht mehr merken.

Vierter Schritt ist die „Zweifaktor-Authentifizierung“ (2FA). Oder, wenn das noch nicht sicher genug ist die Mehrfaktor-Authentifizierung (MFA). Wenn man dann einen Zugang (Account) öffnen will, geht das erst, wenn man eine von dort als Antwort versandte Information zusätzlich eingibt. Die kann per SMS, oder E-mail auf das Mobiltelefon versandt werden, eben auf einem zweiten Kanal den Benutzer erreicht und damit noch sicherer stellt, dass er selbst den Zugang will, oder den Auftrag erteilt hat, sobald er diese Information beim Zugang (Account, Konto, E-mail) eingeben hat. Das Gleiche kann auch eine Authentifizierungs-App leisten, die eine Zeichenkette erzeugt. Für die Mehrfaktor-Authentifizierung könnte man biometrische Merkmal, wie Fingerabdruck, Iris, oder Gesicht benutzen. Auch der Standort des Gerätes kann als Merkmal benutzt werden. Allerdings kommt es vor, dass das eigene Gerät einen nicht mehr am Gesicht erkennt, wenn man zum Beispiel eine Brille auf hat, oder man den Bart abrasierte.

Noch sicherer wird es, wenn man im fünften Schritt „Passkeys“ installiert und benutzt. Dabei wird ein digitales Schlüsselpaar erzeugt. Einer bleibt beim Benutzer, der Andere geht – ebenfalls verschlüsselt - zum Account und nur gemeinsam funktionieren sie. Passkeys wird voran getrieben von der Fido Allianz (<https://fidoalliance.org/members/>), die es ermöglichen will, dass man auf Passwörter verzichten kann, weil Passkeys für ganz viele Account oder Seiten funktionieren soll.

Offenbar hat man gemerkt, dass die Benutzer des Internets keine Lust haben sich mit Dutzenden, wenn nicht Hunderten von Passwörtern herum zu schlagen, auch, wenn das oft automatisiert geschieht.

Andererseits haben Kriminelle und Geheimdienste in Laufe der Zeit hinzu gelernt, was die Risiken für die Benutzer erhöht hat. Dabei hatte man anfangs stets behauptet, das jeweilige Verfahren, zum Beispiel PIN und TAN für das Online-Konto, sei sicher.

Heute muss man davon ausgehen, dass die eigenen Daten gestohlen worden sein könnten. Ob das der Fall ist kann man hier [Have I Been Pwned: Check if your email address has been exposed in a data breach](https://haveibeenpwned.com/) (Sind E-mail-Adresse oder Daten in einem Datenleck aufgetaucht.) überprüfen: (<https://haveibeenpwned.com/>). Bei über 1,3 Milliarden gestohlener Adressen im Darknet ist es gut möglich, dass man betroffen ist.

Allerdings meinte schon vor Jahrzehnten der englische Computerfachmann Paul Liller†, das jeder Besucher des Internets in Gefahr ist, seine Daten zu verlieren, vorausgesetzt jemand sei bereit dafür genügend Geld zu bezahlen, oder den entsprechenden Aufwand zu betreiben. Da erhebt sich die Frage, ob der oben beschriebenen Aufwand sich überhaupt lohnt, oder ob das Internet in Zukunft so herunter gekommen sein wird, dass man es nur noch mit äußerster Vorsicht benutzen kann. Kurz, es ist wahrscheinlich, dass das Internet wegen des steigenden Aufwandes für die Sicherheit an Nutzen und Beliebtheit verliert.