Hinweise zum Umgang mit Passwörtern

Montag, 22 Juli 2019

https://www.datenschutz.de/hinweise-zum-umgang-mit-passwoertern/

Passwortsicherheit ist ein zentrales Thema bei technisch-organisatorischen Datenschutz-Maßnahmen. Die Anmeldung mittels Nutzername und Passwort an zum Beispiel Computern, bei Web-Diensten, Internet-of-Things- bzw. Smart-Home-Geräten stellt das gängigste Verfahren zur Authentifizierung dar. Diese Authentifizierungsmethode ist damit oftmals das wesentliche oder gar einzige Sicherheitselement, das vor dem Zugriff durch Unbefugte schützt.

Rechtliche Grundlage

Die Authentifizierung mittels Nutzername und Passwort sowohl bei Geräten als auch Diensten stellt eine technische und organisatorische Maßnahme nach Artikel 32 der Datenschutz-Grundverordnung (DS-GVO) dar. **Eine sichere Authentifizierung der Nutzer ist ein Baustein, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten, Systeme und Dienste auf Dauer sicherzustellen** (vgl. Art. 32 DS-GVO). Setzen Verantwortliche unzureichende technische und organisatorische Maßnahmen um, können Bußgelder verhängt werden (vgl. Art. 83 Abs. 4 DS-GVO). Verantwortliche sind also angehalten, angemessene technische und organisatorische Maßnahmen durchzuführen.

Hinweise zur Auswahl von Passwörtern

Ein Risiko bei der Verwendung von Passwörtern ist, dass diese von Dritten ermittelt werden können. Daher sind einerseits **die Nutzer selbst in der Pflicht, sichere Passwörter auszuwählen**, andererseits müssen auch Hersteller und Administratoren sichere Vorgaben machen, Passwörter sicher speichern und moderne Techniken anbieten.

Für die Auswahl von sicheren Passwörtern haben sich **eine Reihe von Regeln und Grundsätzen** etabliert. Weitere Informationen, insbesondere, wie Sie selbst ein sicheres Passwort auswählen können, finden Sie unter diesen Links bei unseren Projektpartnern [1, 2].

1. Je mehr Zeichen ein Passwort enthält, desto sicherer ist es.
2. Ein Passwort sollte aus einer zufälligen Kombination von Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.
3. Passwörter sollten keine Namen von Familienmitgliedern, Bekannten, Freunden, Prominenten, Fußballvereinen und dergleichen sowie keine Wörter enthalten, die im Wörterbuch stehen.
4. Eine Eselsbrücke kann helfen, das Passwort zu erinnern.
5. Für verschiedene Dienste sollten verschiedene Passwörter verwendet werden.
6. Passwörter sollten regelmäßig geändert werden.
7. Passwörter sollten nicht an Dritte herausgegeben werden.

Für den Fall, dass Nutzer sich viele Passwörter merken müssen, können diese hierzu ein **Passwort-Verwaltungsprogramm** nutzen. Für dieses Programm ist wiederum ein sicheres Passwort notwendig, da

es für die Sicherheit der Anmeldedaten einen zentralen Angriffspunkt darstellt.

Diese Einführung ist auf Basis der Texte „Hinweise zum Umgang mit Passwörtern“ des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg und „Passwortsicherheit“ der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen entstanden. Für ausführlichere Informationen können Sie unter den folgenden Links recherchieren.

Weiterführende Links

„Selbstdatenschutz: Rund um Ihre PC-Nutzung und Sicherheit“ bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit

„Dossier zum Selbstdatenschutz“ bei dem Landesbeauftragten für Datenschutz und die Informationsfreiheit Rheinland-Pfalz

„Passwortvergabe, -wahl und -verwaltung“ bei dem Bayerischen Landesbeauftragte für den Datenschutz

„Passwörter“ beim Bundesamt für Sicherheit in der Informationstechnik