SICHER IN DER DIGITALEN WELT UNTERWEGS – FÜR EINSTEIGER

Literatur / Quellenhinweise

WWW-Seite mit weiteren Erläuterungen https://**wmcivis.de/verbraucherbildung/**

Weitere Quellenangaben auf der Rückseite …

Hinweise / Empfehlungen

- Ein Aspekt der **digitalen Unversehrtheit** (digitale Integrität) ist die „**IT-Sicherheit**“. Deren klassische Schutzziele sind **Verfügbarkeit** (Geräte und Daten sind vorhanden und funktionsfähig), **Integrität** (reale Sachverhalte werden korrekt abgebildet) und **Vertraulichkeit** (Daten gelangen nur Befugten zur Kenntnis).
- **Zugangsdaten** (Benutzernamen **und** Kennworte) sind **begehrte Ziele von Kriminellen**.
- "**Kennwort**", "**Passwort**" (engl.: password), "**Schlüssel**" (engl.: key) oder "**PIN**" haben i. W. die gleiche Bedeutung und dienen i. d. R. zusammen mit einem **Benutzernamen** als Zugangsdaten der **Sicherung** von **Zugangssystemen** von Online-**Konten** (engl. account).
- Moderne Computer aller Größen (vor allem Mobilgeräte) sind unter **sicheren Betriebsbedingungen** bereits gut geschützt. Dazu gehören die Installation von Sicherheitsupdates des Betriebssystems und App-Updates, Bezug von Apps nur aus sicheren Quellen, Verschlüsselung der Geräte, guter Zugangsschutz sowie regelmäßige Datensicherung (engl.: backup).
- Viel **größere Gefahr** droht unseren Daten während der Übertragung über das Internet, auf Systemen der **Diensteanbieter** sowie von Systemen **anderer Menschen**, mit denen wir **kommunizieren**. Seien Sie **zurückhaltend** mit der **Weitergabe** von Daten zur Erreichbarkeit, vor allem **Mobiltelefonnummern**, aber auch E-Mail-Adressen oder anderen Adressangaben.
- Die **größte Gefahr** droht unseren Daten **durch uns** selbst: durch versehentliches oder unwissentliches Handeln, **Bequemlichkeit**, „**Sparen**“ an der falschen Stelle, fehlende Absicherung von Schadensfällen sowie Unterschätzen der Tatsache, dass diese „Verwundbarkeit“ von Kriminellen am leichtesten ausgenutzt werden kann und am häufigsten ausgenutzt wird.
- Sichern Sie Ihre Daten nach der **3 – 2 – 1 Reg**el (3 Datenbestände (Original + 2 Kopien) – auf 2 unterschiedlichen Medien – davon 1 Bestand / Kopie außer Haus)
- Nutzen Sie sog. „**Passwortmanager**“ (Kennwort-/Identitätsverwaltung), mit denen Sie eine Vielzahl von Zugangsdaten (**Benutzerkennungen und Kennwörtern**) speichern können. Diese Anwendungen sind darüber hinaus **bequem** bei der Eingabe der Zugangsdaten.
- Je **größer** die **Zahl** der verwendeten **Benutzerkennungen und Kennwörter**, umso **geringer** der **Schaden**, wenn die Zugangsdaten eines Dienstes offengelegt oder ausgenutzt werden. Verwenden Sie für **jeden Dienst** ein **eigenes Kennwort**, **besser sogar eine eigene Benutzerkennung**.
- Sie müssen Kennwörter **nicht regelmäßig ändern**; nicht jeder Dienst hat **gleich hohe Sicherheitsanforderungen**; Sie können die Sicherheit von Kennwörtern häufig selbst **bedarfsangemessen** festlegen. Erstellen Sie ein **Konzept**, **dokumentieren** es und halten Sie sich **strikt** daran. Denken Sie an Abwesenheit, Unfälle, Krankheit … sowie den **digitalen Nachlass**.
- Nutzen Sie (bedarfsangemessen) **komplexe Kennwörter** (keine Eigennamen, Spitznamen, Kosewörter oder Zitate; verwenden Sie verschiedene Zeichen in Groß- und Kleinschreibweise, Sonderzeichen und Zahlen). Übliche Längen sind 8 – 12 Zeichen, mehr Zeichen sind jedoch besser.

- **Informieren** Sie sich regelmäßig bei den Verbraucherzentralen, dem Bundes- und den Landesbeauftragten für den Datenschutz, der Polizei, dem BSI, Themendiensten im WWW (z. B. mobilsicher.de oder klicksafe.de), gerne unter https://wmcivis.de und vielen weiteren Stellen (s. Linkliste).

Prüfung, ob Kennwörter oder Identitäten bereits missbräuchlich verwendet wurden

An verschiedenen Stellen können Sie überprüfen, ob Ihr Kennwort oder Ihre Identität (E-Mail-Adresse oder Telefonnummer) bereits durch eine Sicherheitslücke oder einen Angriff von Kriminellen erbeutet wurde. Seien Sie trotzdem misstrauisch. Wenn Ihre Zugangsdaten nicht als in der Datensammlung hinterlegt (engl.: pawned) angezeigt werden, können sie trotzdem bereits missbräuchlich verwendet worden sein**.**

- Kennwörter bzw. Identitäten https://haveibeenpwned.com/passwords
- Weitere Quellen https://wmcivis.de/sicher-in-der-digitalen-welt /

Kennwort- / Identitätsverwaltung („Passwortmanager“)

https://wmcivis.de/#pwmanager

Dies sind Anwendungen oder Dienste, die Sie bei der Verwaltung von Zugangsdaten und bei der automatischen Anmeldung unterstützen können. Im Internet laufende Dienste sind sehr bequem zu nutzen, stellen angesichts der hohen Zahl dort gespeicherter Daten aber auch ein attraktives Ziel für Kriminelle dar. Zugangsdaten mit sehr hohem Schutzbedarf (z. B. für Zahlungsabwicklung oder Kommunikationsdienste) sollten daher eher lokal, an sicherer Stelle gespeichert werden.

Passkeys – Nie wieder Kennworte eingeben?

Die Anforderungen an die Sicherheit von Kennwörtern steigen in dem Maße, wie Kriminellen hoch leistungsfähige Computersysteme zur Verfügung stehen, um - vereinfacht gesagt, durch "ausprobieren" - Kennwörter offenzulegen. Kennwort- und Identitätsverwaltungen erlauben zwar den Einsatz vieler unterschiedlicher Identitäten und komplexer Kennworte, erfordern jedoch Koordinationsaufwand und sind zuweilen unbequem. Passkeys können die Nachteile der Authentifizierung mit Kennwörtern bei Onlinediensten teilweise ausgleichen, erfordern jedoch auch Verständnis über ihre Arbeitsweise und einen gewissen Koordinierungsaufwand. Außerdem setzen bisher nur wenige Anbieter solche Verfahren ein. Die Anmeldung mit Benutzerkennung und Kennwort wird noch einige Zeit die Regel sein.
(siehe auch: https://wmcivis.de/passwortschutz-und-datensicherheit/#passkey)

Weitere Quellen

siehe auch https://wmcivis.de/linkliste-dienste

Warnungen vor und Hinweise zu Fake-Shops und Phishing-Angriffen bei Verbraucherzentralen und anderen Einrichtungen	www.verbraucherzentrale-niedersachsen.de/vorsicht-falle www.watchlist-internet.at www.vz-bw.de/node/13166
Informationen des Bundesamtes für Sicherheit in der Informationstechnik - BSI	www.bsi-fuer-buerger.de
Klicksafe - EU-Initiative, u.a. mit dem Ziel, die Online-Kompetenz der Menschen zu fördern	www.klicksafe.de
„Digitale Selbstverteidigung“ bei digitalcourage	digitalcourage.de/digitale-selbstverteidigung

Zu allen hier erwähnten Themen finden Sie weitere Hinweise und Erläuterungen unter **https://wmcivis.de**.

Die wesentlichen Inhalte des Vortrags sowie Quellenangaben und Links zu weiterführenden Themen finden Sie unter **https://wmcivis.de/verbraucherbildung**

https://wmcivis.de/ https://wmcivis.de/linkliste-dienste