A & O

Sicherheit hat Priorität

Überblick

Android oder IOS

Alpha und Omega (A und O), der erste und der letzte Buchstabe des klassischen griechischen Alphabets, sind Symbol für Anfang und Ende, für das Umfassende.

Transferiert in die heutige digitale Welt kann es stehen für:

*Starke Passwörter verwenden **und** Ersatzschlüssel bereithalten.*

Sehr wichtig, der Zugriff zum Smartphone (Handy) oder Tablet muss immer mit einem Zugang (Pin, Muster, Fingerprint, Gesichtsscan etc.) gesichert sein.

Passwörter- lästig? ABER doch sehr wichtig!

(Lästig- jemand in unangenehmer Weise beanspruchen, störend, ihn in seinem Tun behindernd).

In den Medien häufen sich Berichte über die großen Fälle, Konten werden ‚gehackt', Daten werden ausgespäht und missbräuchlich genutzt. Dabei kann es jeden von uns treffen, jeden Tag. Beispiele werden im Vortrag gezeigt.

- ➔ *Es wird versucht Zugriff zum E-Mail-Konto zu erlangen.*
  Übersicht im E-Mail-Konto.
- ➔ *Kleinanzeigen Konto wird durch illegalen Zugriff missbraucht.*
  Warnhinweis durch Plattformanbieter.
- ➔ *Passwort oder andere Daten wurden ausgespäht.*
  Lässt sich prüfen mittels Identity Leak Checker.

Wir empfehlen den Internetauftritt des **Bundesamts für Sicherheit in der Informationstechnik** zu studieren.

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Setzten Sie immer möglichst sichere Passwörter.

Mindestens 12 Zeichen lang, verwenden Sie Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.

Soweit- so gut.

Wer kennt es nicht, sehr lange nicht genutzt und jetzt wird es gefordert--wie war nochmal mein Passwort?

Ein paarmal falsch eingegeben (je nach Anwendung schon bei 3x) und der Zugriff ist gesperrt.

Der Passwort Wiederherstellungsprozess wird aktiviert. Alles kein Problem, wenn die Wiederherstellungsdaten (Ersatzzugang zum Konto) ordentlich gesetzt sind. Für Ihren Wohnungseingang haben Sie ja auch einen Ersatzschlüssel.

Falls nicht wird es schwierig bis unmöglich wieder Zugriff zu erlangen.

Es gab schon Beispiele wo der Zugang zu einem E-Mail-Konto, von einem bekannten Telekommunikationsunternehmen, nur über die Festnetzanschluss-Kennung, die vor 40 Jahren mitgeteilt wurde, schriftlich via Post wieder hergestellt werden konnte.

Übrigens, diese Wiederherstellungs- und Kontaktdaten betreffen nicht nur Handy oder Tablet. Sie sind genauso hilfreich bei Windows / Microsoft Umgebungen.

Die Wiederherstellungs- und Kontaktdaten sollten wo immer möglich eingerichtet und auch notiert sein, besonders bei

- Microsoft / Windows
- Google Konto
- E-Mail-Konto

Der Vollständigkeit halber, für Bankkonten, Bankkarten, Kreditkarten usw. gibt es Sperr-Telefonnummern, welche 24 Stunden erreichbar sind, falls es fremde Bewegungen auf dem Konto gibt.

Glücklich kann sich schätzen wer nur zwei, drei Passwörter sein Eigen nennt.Oft sind es 20, 30 oder mehr Passwörter die gesetzt sind. Im Laufe der Zeit kommt einiges zusammen. Niemand kann sich so etwas merken. Also aufschreiben. Damit diese Listen in falschen Händen nicht genutzt werden können, sollten die aufgeschriebenen Passwörter immer auch einen geheimen Teil haben. Der für alle PW gleich sein kann, weil geheim. Dieser geheime Teil kann jedem PW vor- oder nachgesetzt werden oder zwischendrin, z.B. immer ab 3.Stelle.

Beispiele:

Geheimer Teil a#=7St PW: 7BrZG64%/de79&%

a#=7StZG64%/de79&%

oder

PW: ZG64%/de79&% geheimer Teil a#=7St

ZG64%/de79&%a#=7St

Geheimer Teil / öffentlicher, aufgeschriebener Teil des Passworts

a#=7St ZG64%/de79&%

a#=7St zZTGV)*59Txc

usw…….

Der geheime Teil ist frei wählbar, sollte merkbar sein (**a**m **#**Zaun **=**sind **7St**ickel) und natürlich nicht leicht zu erraten.

Falls das **Passwort vergessen** wurde ist der ‚Passwort vergessen' Prozess zu starten. Dazu werden die Wiederherstellungs- und Kontaktdaten genutzt.

Sehen Sie dazu auch die Unterlage ‚E-Mail-Konto Wiederherstellung einrichten' auf unserer Internetseite.

Ist Ihr verwendetes Passwort sicher? Tests werden in den Sicherheitseinstellungen vom Google-Konto oder Ihrem E-Mail-Konto angeboten.

Verwendete Passwörter sind wo abgelegt oder **einsehbar**? Verschaffen Sie sich einen Überblick z.B. im Google Passwortmanager oder im Browser unter Passwörter.