Sicheres Passwort erstellen und anwenden

In der heutigen Zeit wird fast immer eine Zugangskennung und Passwort benötigt um beispielsweise in einem Onlineshop zu bestellen, Onlinebanking durchzuführen, um seinem Sozialmedia Account nutzen zu können, oder auch um sich als Administrator bzw. "normaler Benutzer" an ein bzw. sein CMS anzumelden.

Der Accountname (Benutzerkennung) ist oftmals durch die Anwendung vorgegeben und somit kommt dem Passwort eine umso größere Bedeutung zu, die eigenen Daten bzw. Rechte vor dem unberechtigten Zugriff durch Dritte zu schützen.

Mit einem "geknackten Passwort" könnte der Angreifer beispielsweise das Girokonto bis zum Dispolimit ausreizen, oder mit ihrem Sozialmedia Account Mobbing durchführen, oder ihre privaten Bilder aus der Cloud sind für alle in einem Datingportal sichtbar.

Eine Anleitung zum Ändern des CMSimple_XH Passwortes befindet sich in der Onlinedokumentation von CMSimple_XH (Link auf das entsprechende Kapitel in der 1.6-er CMSimple_XH Dokumentation).

Anleitung für die Erstellung eines sicheren Passwortes:

- Keine einfachen bzw. zusammengesetzten Wörter verwenden, die im Wörterbuch zu finden sind.
- Niemals den Accountnamen (Benutzernamen) als Passwort (Kennwort) verwenden.
- Keine einfachen (fortlaufende) Zeichen- bzw Ziffernketten von der Tastatur verwenden.
- Keine Namen von Menschen, Tieren, Städten, Ländern, ... verwenden.
- Keine Zahlenkombinationen des Geburtsdatums, Telefonnr., Karten-PIN, ... verwenden.
- Keine zu einfache Struktur bzw. Aufbau eines Passwortes verwenden, damit mit einem geknackten Passwort nicht die Passwörter anderer Anwendungen, Accounts, ... daraus abgeleitet werden können.
- Es sollte aus Groß- und Kleinbuchstaben sowie Zahlen bestehen und idealer weise auch (zugelassene) Sonderzeichen enthalten
- Es sollte aus mindestens 8 Zeichen bestehen, da kurze Passwörter schneller ermittelt werden.
- Das Passwort kann beispielsweise aus einem Satz gebildet werden, indem die x-te Stelle der Wörter bzw. Zahlen verwendet wird, da das Passwort sich mit der Eselsbrücke aus dem Satz leichter zu merken ist.

Anwendung des sicheren Passwortes:

- Vorgegebene Passwörter (Default- bzw. Initialpasswort) sofort ändern.
- Das Passwort regelmäßig ändern
- Schon einmal verwendete Passwörter nicht noch einmal verwenden.
- Für jeden Dienst, Anwendung, Account, ... ein anderes Passwort verwenden.
- Passwort "im Kopf" haben, nicht unverschlüsselt speichern, bzw. aufschreiben und sichtbar ablegen.
- Falls man sich ein langes und kompliziertes Passwort nur schlecht merken kann, könnte dieses mit einer "Umschreibung" (also nicht das eigentliche Passwort) als "Gedankenstütze" auf einem Blatt Papier notieren, welches Dritten nicht zugänglich gemacht wird.
- Die Benutzerkennung und das Passwort sollte möglichst nur über eine gesicherte Verbindung übertragen werden.
- Keiner anderen Person das Passwort mitteilen.
- Die Eingabe des Passwortes vor den Blicken anderer Personen bzw. Kameras schützen.
- Passwörter nach Möglichkeit nicht an einem fremden PC, Notebook, ... eingeben.
- Keine automatische Speicherung der Zugangsdaten zulassen (Browsereinstellung).
- PC, Notebook, Tablet und Smartphone durch ein Passwort vor dem unberechtigten Zugriff schützen.
- Eine Firewall zwischen dem Internet und dem genutzten PC, Notebook, ... erhöht den Schutz der genutzten Hardware (PC, ...) und erschwert einen Passwortangriff. (In den meisten Routern ist eine Firewall als "Hardwarelösung" schon enthalten, die einen besseren Schutz als eine Firewals als Softwarelösung auf dem PC bietet.)
- Eine aktuelle Antivirus-Software auf dem genutzten PC, Notebook, ... hilft mögliche "Schnüffelprogramme" (Keylocker) zu finden.
- Vor der Eingabe des Acounts und Passwortes sollte die Loginseite auf ihre Echtheit und Originalität prüfen,

damit die Zugangsdaten nicht auf einer gefakten (gefälschten) Loginseite eingegeben werden (Pishing). Indizien für eine gefakte Loginseite sind:

- Der Link zur Loginseite wurde per Mail zugesendet.
- Die URL entspricht nicht dem gewöhnten (bekannten) Internetadresse.
- Das Layout (Anordnung und Farbe) und Text (ungewöhnlicher Schreibstil und Rechtschreibfehler) sind anders als von Original gewohnt

Für die Erstellung und Nutzung eines verschlüsselten Passwortes werden im Internet auch einige Lösungen angeboten, die hier beispielhaft aufgeführt sind:

https://www.ines-datenschutz.de/datenschutz-ines-ag/info-seite-3/

Anleitung Passwortkarte

KeePass Password Safe

Falls in dieser Anleitung einige sicherheitsrelevante Aspekte fehlen sollten, werden diese gern hinzugefügt.

```
Hartmut Keil - http://cmsimplexh.webdesign-keil.de - Stand: 01.10.2015
```