EINLEITUNG *Selbststudium*

Massvorsätze

SI-Präfixe: [T] → Tera → 10^{12} → 1'000'000'000'000 → Billion
[G] → Giga → 10^{9} → 1'000'000'000 → Milliarde
[M] → Mega → 10^{6} → 1'000'000 → Million
[k] → kilo → 10^{3} → 1'000 → Tausend

IEC-Präfixe: [Ti] → Tebi → 2^{40} → 1'099'511'627'776
[Gi] → Gibi → 2^{30} → 1'073'741'824
[Mi] → Mebi → 2^{20} → 1'048'576
[Ki] → Kibi → 2^{10} → 1'024
IEC-Präfixe nur im Zusammenhang mit Speichergrössen!

Bit/Byte: Bit = **B**inary dig**it**
8 Bit = 1 Byte
16 Bit = 1 Word
Abkürzung für Bit = b
Abkürzung für Byte = B

HEX: HEX: Hexadezimalsystem, Sechzehnersystem, MAC-Adressen, IPv6
Zeichen: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A (10), B (11), C (12), D (13), E (14), F (15)
(*Eine Hex-Ziffer = vierstelligen Dualzahl oder 4 Bit*)

Sichere Passwörter

Das 100% sichere Passwort gibt es nicht, weil mit genügender Rechenleistung und Zeit «Bruteforce» sich jedes Passwort knacken lässt. Vielmehr geht es darum, es einem Cyberkriminellen mit «123456», «Password», «Pa$$w0rd», «admin», «qwertz», «monkey» oder sonstigen Wörterbucheinträgen nicht allzu einfach zu machen.

Was zeichnet ein sicheres Passwort aus?

- Passwortlänge
- Verwendung von Buchstaben, Zahlen, Sonderzeichen
- Zufällige, sinnlose Anordnung von Buchstaben und Zahlen
  Tipp: Anfangsbuchstaben eines ihnen bekannten Satzes verwenden.
- Gross- und Kleinbuchstaben, vorteilhafterweise innerhalb des Passworts
- Sonderzeichen, vorteilhafterweise innerhalb des Passworts. Nicht nur «!» oder «?».
- Für verschiedene Anwendungen verschiedene Passwörter erstellen
- Delegieren der Passwortwahl und Verwaltung an einen Passwortgenerator/Passwortmanager

Was ist bei Passwort-Manager/Generatoren zu beachten?

- Internetbrowser mit «eingebauten» Passwort-Manager können unter Umständen unbemerkt von Cyberkriminellen abgegriffen werden.
- Wenn Passwörter von z.B. Apples- und Googles Passwort-Manager auf ausländischen Servern gespeichert werden, können allenfalls Geheimdienste darauf zugreifen. (USA: Cloud-Act).

- Nutzung eines lokalen Passwort-Managers, wo Passwörter auf dem eigenen Speichermedium gespeichert werden wie z.B. bei der Open-Source Lösung KeePass. Allerdings verliert man beim Verlust des Speichermediums auch seine Passwortdatenbank und damit seine Passwörter. Darum regelmässige Backups!
- Nutzung eines Passwortmanagers der die Passwörter Ende-zu-Ende verschlüsselt abspeichert, wie z.B. die OpenSource Lösungen Bitwarden oder Padloc, deren Sicherheit unabhängig überprüft wurde.

Wie sicher ist ihr Passwort? Hier zum Beispiel kann man dies überprüfen:
https://www.cryptool.org/de/cto/password-meter

Softwarepflege

- **Patchday** ist ein inoffizieller Begriff für einen Zeitpunkt, an dem ein Unternehmen wie z.B. Microsoft gesammelt Softwareaktualisierungen (**Patches**) für seine Produkte veröffentlicht.
- Unter **Update** (Softwareaktualisierung) versteht man in der IT die Aktualisierung von Software wie z.B. das **Betriebssystem** (Operating-System), **Applikationen**, aber auch **Virensignaturen** oder Datenbanken, Websites etc. oder das Update einer Dokumentation, eines Berichts.
  Aber auch die PC-System-**Firmware** (BIOS, UEFI) oder die HW-**Treiber** für Grafikkarte, Festplatte, SSDs, optische Laufwerke etc. müssen hin und wieder upgedatet werden.
- Nicht aktualisierte, veraltete SW kann zum **Sicherheitsrisiko** werden.

Backup

Backup oder Datensicherung bezeichnet den Vorgang zum Sichern von Daten mit der Absicht, diese im Falle eines Datenverlustes wiederherzustellen.
Die auf einem Speichermedium redundant gesicherten Daten werden als Sicherungskopie oder als Backup bezeichnet, die entweder online oder offline angelegt werden kann. Die Wiederherstellung der Originaldaten aus einer Sicherungskopie bezeichnet man wiederum als Datenwiederherstellung, Datenrücksicherung oder **Restore**.

Bei der Datensicherung ist es sehr wichtig, eine **gute Dokumentation** (Datenbank) zu führen, da von ihr der Erfolg und die Geschwindigkeit der Datensicherung sowie der Wiederherstellung abhängen können.

Je nach Veränderungsintensität der zu sichernden Daten können beim Backup **verschiedene Sicherungsarten** eingesetzt werden.

- **Fullbackup**: Mindestens wöchentliche Sicherung aller Daten.
- **Differenzielles Backup**: Es werden mindestens täglich nur die seit dem letzten Fullbackup veränderten Daten gesichert.
- **Inkrementelles Backup**: Es werden mindestens täglich nur die seit dem letzten inkrementellen Backup oder Fullbackup veränderten Daten gesichert.

Um bei Diebstahl, Brand- oder Wasserschaden etc. nicht Original (PC, HD) und Backup zu verlieren, sollen diese **örtlich getrennt** aufbewahrt werden.

Spiegelung und/oder Stripping des Speichermediums (**RAID**) ersetzt **kein Backup**!