Das Passwort

Warum ein sicheres Passwort?

Ein sicheres Passwort schützt

- den PC vor unbefugtem Gebrauch
- Online-Accounts (E-Mail, …) vor „Fremden“
- vor der Erfassung persönlicher Daten durch Fremde

Welche Passwörter sind nicht sicher?

- Alle Wörter aus dem Duden
- Alle Namen
- Alle real existierenden Wörter
- Alle fortlaufenden Tastenfolgen der Tastatur

Wie ist ein sicheres Passwort aufgebaut?

Kombination aus

- Kleinbuchstaben
- Großbuchstaben
- Zahlen
- Sonderzeichen
- Mindestens 8 Zeichen lang

Was ist sonst noch wichtig?

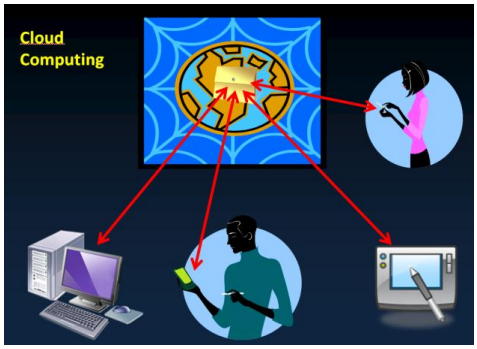
- Nicht das gleiche Passwort für alle Anwendungen verwenden.
- Passwörter regelmäßig ändern (aber nicht durch z.B. aufsteigende Ziffern – 1Ghrt*65, 2Ghrt*65, 3Ghrt*65
- Passwort nie unverschlüsselt speichern
- Anzahl der „Mitwisser“ gering halten
- Passwortliste (analog) zur Sicherung an geschütztem Ort aufbewahren.

Software

- Software selbständig aktualisieren lassen um Sicherheitslücke zu schließen (Betriebssystem, Anwendungssoftware, Virenschutz).
- Nur legale Software seriöser Anbieter verwenden.

Cloud Computing

Cloud Computing - Bedrohungen



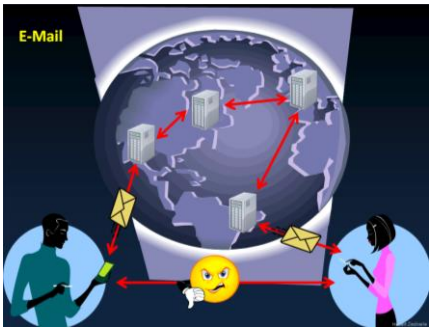
- Cloud Angebote und ihre Verwaltungsdienste / Programmschnittstellen sind über das Internet erreichbar und deswegen leicht angreifbar (um z.B. Zugriff auf Kundendaten zu bekommen).
- Sind die Mitarbeiter des Cloud-Anbieters absolut zuverlässig?
- Werden die Daten der Cloud-Nutzer zuverlässig getrennt?
- Unbekannte neue Risiken?

Cloud Computing - Sicherheitsrisiken

- Es ist keine Lokalisierung der Daten möglich!
- Werden die Daten bei einer Löschung wirklich gelöscht?
- Werden deutsche Datenschutzbestimmungen eingehalten (in welchen Ländern stehen Server)?
- Was passiert bei Insolvenz des Providers mit den Daten? Werden diese verkauft?
- Beauftragt der Cloud-Anbieter Subunternehmer?
- Tauschen verschiedene Anbieter untereinander Daten aus?

Es ist davon auszugehen, dass alle einmal im „Netz“ gespeicherten Daten für immer „irgendwo“ gespeichert werden!
(mit Anmeldeinformationen, IP-Nummer, Standort, …)

E-Mail



Die **E-Mail** („elektronische Post“) ist eine auf elektronischem Weg in Computernetzwerken übertragene, briefähnliche Nachricht.
Authentizität: Die E-Mail stammt wirklich vom Absender (Original und keine betrügerische Fälschung).
Datenschutz: Schutz vor Mitlesen durch Dritte auf dem Übertragungsweg.
Integrität: E-Mail-Inhalt bleibt bei der Übertragung vollständig und unverändert.
Die **unverschlüsselte E-Mail** (Standard) ist vergleichbar mit einer Postkarte.
Der ganze Inhalt ist für jeden auf dem Transportweg (u. U. um die ganze Welt) lesbar.
Vom E-Mail-Dienstleister werden Kopien gemacht und eine Zeit lang aufbewahrt.

Es ist davon auszugehen, dass alle einmal im „Netz“ versandten Daten für immer „irgendwo“ gespeichert werden!
(mit Sender- Empfängerinformationen, Inhalt, …)