Sichere Passwörter und deren Verwaltung

PC-Treff-BB
Ingolf Wittmann
10. Mai 2014

Übersicht

- Pins, Tans, Passwörter
- Was sind sichere Passwörter
- Passwort Management
- Single Sign On
- Tools
- Demo
- Quellen

Gefahren

- Cookies speichern beliebige Informationen (u.a. auch Passwörter)
- Es gibt verschiedene Möglichkeiten um Passwörter zu knacken
  - a) Wörterbuch-Angriff
  - b) Brute-Force-Attacken
- Unverschlüsseltes Übertragen von Passwörtern
- Dasselbe Passwort mehrfach verwenden
- Single Sign On mit Google, Facebook & Co

Brute Force Angriff

Rechenzeit eines Brute-Force-Angriffs bei 1 Milliarde Schlüsseln pro Sekunde

	Passwortlänge								
Zeichenraum	**4 Zeichen**	**5 Zeichen**	**6 Zeichen**	**7 Zeichen**	**8 Zeichen**	**9 Zeichen**	**10 Zeichen**	**11 Zeichen**	**12 Zeichen**
10 [0-9]	<1 ms	<1 ms	1 ms	10 ms	100 ms	1 Sekunde	10 Sekunden	2 Minuten	17 Minuten
26 [a-z]	<1 Sekunde	<1 Sekunde	<1 Sekunde	8 Sekunden	4 Minuten	2 Stunden	2 Tage	42 Tage	3 Jahre
52 [A-Z;a-z]	<1 Sekunde	<1 Sekunde	20 Sekunden	17 Minuten	15 Stunden	33 Tage	5 Jahre	238 Jahre	12.400 Jahre
62 [A-Z;a-z;0-9]	<1 Sekunde	<1 Sekunde	58 Sekunden	1 Stunde	3 Tage	159 Tage	27 Jahre	1.649 Jahre	102.000 Jahre
96 (+Sonderzeichen)	<1 Sekunde	8 Sekunden	13 Minuten	21 Stunden	84 Tage	22 Jahre	2.108 Jahre	202.000 Jahre	19 Mio Jahre

Quelle: Wikipedia http://de.wikipedia.org/wiki/Passwort

Sichere Passwörter

Ein gutes Passwort:

sollte mindestens zwölf Zeichen lang sein.

(Ausnahme: Bei Verschlüsselungsverfahren wie z.B. WPA und WPA2 für WLAN sollte das Passwort mindestens 20 Zeichen lang sein. Hier sind so genannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren - das geht z.B. beim Hacken von Online-Accounts nicht.)

sollte aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern (?!%+…) bestehen.

Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten usw.

wenn möglich sollte es nicht in Wörterbüchern vorkommen.

soll nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmusternmustern bestehen, also nicht asdfgh oder 1234abcd usw.

Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? #, am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen ist auch nicht empfehlenswert.

Bitte beachten: Wenn das System Umlaute zuläßt, bei Reisen ins Ausland ist zu bedenken, dass auf landestypischen Tastaturen diese evtl. nicht eingegeben werden können.

Quelle: BSI https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html

Passwortübung

1. CatSonneMusikBMW
2. M=3, i=!, n=8
3. **CatSo88e3us!kB3W**

1. elr%??avz??
2. Www.amazon.de
3. **elr%anavz06**

1. Im Sommer esse ich am liebsten Himbeer Eis!
2. **ISeialHE**

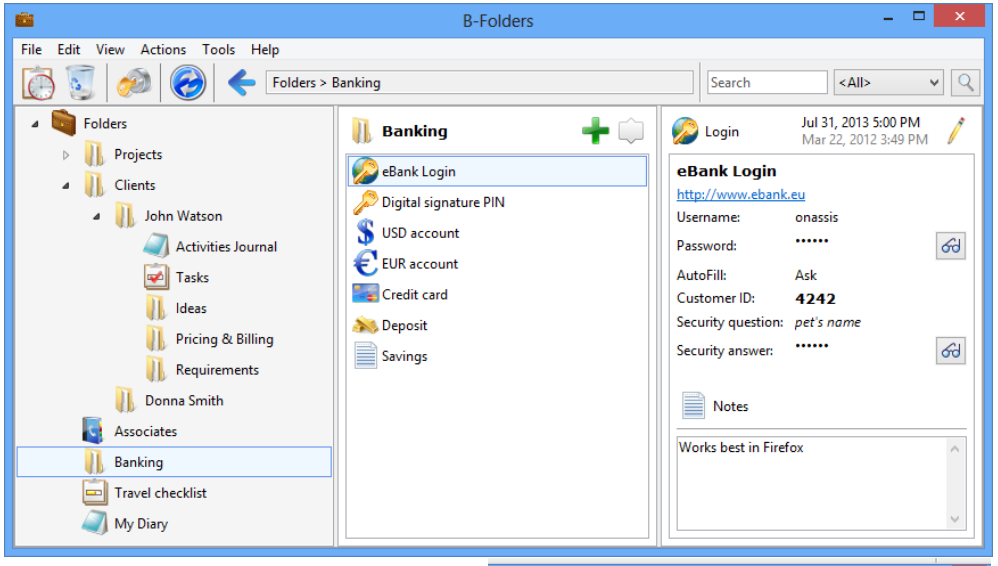
Passwort Verwaltung

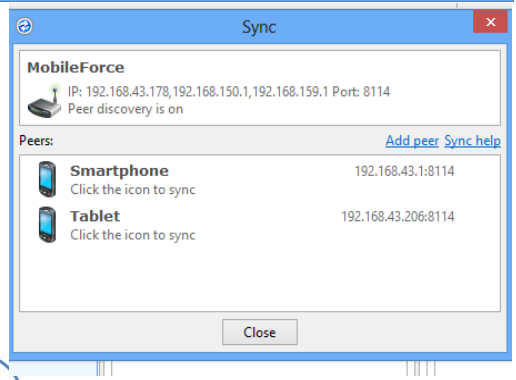
- Verschlüsselte Dateien/Verzeichnisse
  - lokal
  - Dropbox
- Passwortgeschützte Dateien
  - Spreadsheets
- Tools
  - B-Folders
  - TrueCrypt

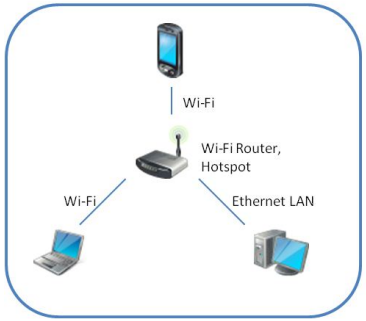
Wo habe ich wie und wann Zugriff auf die Informationen?
→ Offline ?!

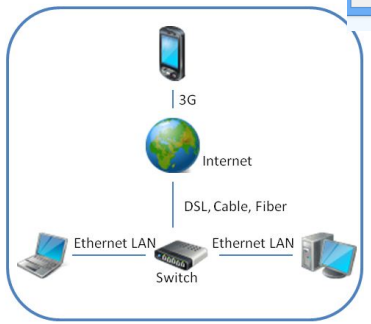
B-Folders

- Für Windows, Mac, Linux, & Android (free)
- Kosten $29,95 + VAT (für 5 Geräte)
- Voll verschlüsselt mit 256-bit AES
- Peer Synchronisation mit TLS in
  - Privaten Netzwerken
  - USB Kabel
- Unterschiedliche Objekte
  - Banken, Kundenkarten, Pins, Passwörter, Dokumente
- Migration von anderen Tools
- Firefox & IE Plugins zum automatischen Logon









PC-Treff-BB
Sichere Passwörter und deren Verwaltung
© 08.05.2014 - Ingolf Wittmann

Demo

Quellen

- http://de.wikipedia.org/wiki/Passwort
- http://de.wikipedia.org/wiki/Kennwortverwaltung
- http://www.heise.de/thema/Passwort
- https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoer
- http://www.jointlogic.com/b-folders/
-
- ct 2009/02 Passwörter mit Köpfchen
- ct 2011/02 Sesam öffne dich nicht