Passwort

-

Sicherheit

13. Juni 2017 / D. Hänni

Passwort-Sicherheit

- ***Agenda***
  - Warum brauche ich ein sicheres Passwort ?
  - Was ist ein sicheres Passwort ?
  - Länge oder Anzahl differierender Zeichen
  - Passwort-Manager
  - Fragen ?

Passwort-Sicherheit

- ***Agenda***
  - Warum brauche ich ein sicheres Passwort ?
  - Was ist ein sicheres Passwort ?
  - Länge oder Anzahl differierender Zeichen ?
  - Passwort-Manager
  - Fragen ?

Passwort-Sicherheit

Warum brauche ich ein sicheres Passwort ?

- 16.05.2017: Forscher der IT-Sicherheitsfirma Kromtech Security Center haben in einer nicht gesicherten MongoDB-Datenbank mehr als 560 Millionen E-Mail-Adressen und Passwörter aus verschiedenen Quellen gefunden.
  (http://t3n.de/news/leak-datenbank-login-daten-823503/)

- Meldungen über PW-Leaks (einige Beispiele aus den letzten Jahren)
  - Adobe 38 Mio. Kundendatensätze
  - LinkedIn, 117 Mio. Konten
  - Twitter, 32 Mio. Zugangsdaten
  - Myspace, 360 Mio. Kennwörter

Passwort-Sicherheit

Warum brauche ich ein sicheres Passwort ?

- Irgendwann kommt jemand an eines eurer Passworte
  (via Hack bei eurem Provider, bei einem Webdienst den ihr verwendet.)
- Hoffentlich waren die Passworte bei diesem Webdienst verschlüsselt als Hashwert gespeichert !
- Aber: Es existieren heute frei verfügbare, bzw. käuflich erwerbbare Rainbowtables, welche Hashwerte und das zugehörige Klartext-Passwort enthalten!
- Verwende ich für viele Webdienste dasselbe Passwort ?
  Wo habe ich das geleakte Passwort jetzt schon wieder überall verwendet ? Welche meiner Zugänge sind nun alle kompromittiert ?
- → Fazit:
  Ihr habt die Sicherheit eurer Passworte nicht (nur) in euren Händen !

Passwort-Sicherheit

- ***Agenda***
  - Warum brauche ich ein sicheres Passwort ?
  - Was ist ein sicheres Passwort ?
  - Länge oder Anzahl differierender Zeichen
  - Passwort-Manager
  - Fragen ?

Passwort-Sicherheit

Was ist ein sicheres Passwort ?

- Mindestens 8 Zeichen
- Klein- / Grossbuchstaben und Sonderzeichen
- Ziffern und Sonderzeichen nicht nur am Anfang oder am Ende des Passworts verwenden

Passwort-Sicherheit

Regeln für ein sicheres Passwort ?

- Nutze für **jeden** Dienst **ein eigenes** Passwort, ausnahmslos!
- Ändere die wichtigsten Passwörter alle 2-3 Monate
  (na ja, macht eigentlich keiner wirklich – ausser, er wird vom Sysadmin gezwungen)
- Nutze für wichtige Dienste 2-Faktor-Authentifizierung (2FA)
  - Heute u.U. einstellbar: nur wenn der Zugriff ab einem neuen System erfolgt, wenn bestimmte Funktionen (PW-Wechsel) ausgeführt werden.
  - Bei eBanking heute schon Standard und auch sinnvoll !
- Btw: 2FA mit ein und demselben Gerät (Smartphone) ist 2FA ad-absurdum geführt !

Passwort-Sicherheit

Was ist ein sicheres Passwort ?

- Beispiele

Passwort	Anzahl Zeichen	Dauer BruteForce-Attacke (normaler Heim-PC)
Z7@iSk!P	8	ca. 12 Tage
Zr7@iSk!P	9	ca. 4 Monate
Zr7@iS0k!P	10	ca. 4 Jahre

Quelle: https://password.kaspersky.com/de/

- → Noch blöd, ich kann mir solche Passworte einfach nicht merken !
- → Aufschreiben ? – ist schon schwierig, Abtippen dann auch.
- BruteForce: Theoretische Werte, wenn Angreifer Zugang zum System hat, btw: die NSA hat eine etwas bessere Rechen-power als wir zuhause ;-)

Passwort-Sicherheit

Was ist ein sicheres Passwort ?

- 98% aller Konten, sind mit den 10'000 gängigsten Passwörtern geschützt !

Bemerkung	Passwort	Anzahl Zeichen	Dauer Bruteforce
Hobby	Fussball	8	2 Minuten
Eines der häufigsten Passworte überhaupt	123456	6	1 Sekunde
Auch ab und an verwendet	Passwort	8	39 Sekunden
Vorname	Melanie	7	4 Sekunden
Vorname in Kombination mit Geburtsjahr	Dani1963	8	2 Stunden

Quelle: https://password.kaspersky.com/de/

- → nicht zu empfehlen !

Passwort-Sicherheit

Was ist ein sicheres Passwort ?

- Weitere Beispiele (einfacher zu merken)
  - Erster Satz aus meinem Lieblingsbuch, meinem -Song und einzelne Buchstaben mit Ziffern oder Sonderzeichen ersetzt:

Satz / Songzeile	Passwort	Anzahl Zeichen
Born down in a dead man's town (Born in the U.S.A. – Bruce Springsteen)	B0rn-d0wn-1n-@-d3@d-m@n'5-t0wn	30
Wenn von Computersicherheit gesprochen wird, dann oft in sehr allgemeiner Art und Weise: "Dieses System ist sicher", oder "Wir sichern E-Commerce". (Secret & Lies – Bruce Schneier)	WvCgw,doisaA&W:DSis,oWsE-C.	27

Passwort-Sicherheit

Was ist ein sicheres Passwort ?

- Weitere Beispiele (einfacher zu merken)
  - Kombination aus sicherem Mittelteil und Webseite / -dienst („Ein Neger mit Gazelle zagt im Regen nie“):

Webseite / -dienst	Passwort	Anzahl Zeichen
KeePass	Kee-E1N3m1G@z@1mR3N1-Pass	25
Facebook	Face-E1N3m1G@z@1mR3N1-Book	26
Bluewin	Blue-E1N3m1G@z@1mR3N1-Win	25
Amazon	Ama-E1N3m1G@z@1mR3N1-Zon	24
BKB-ebanking	BKB-E1N3m1G@z@1mR3N1-ebanking	29
Digitec	Digi-E1N3m1G@z@1mR3N1-Tec	25

Passwort-Sicherheit

- ***Agenda***
  - Warum brauche ich ein sicheres Passwort ?
  - Was ist ein sicheres Passwort ?
  - Länge oder Anzahl differierender Zeichen
  - Passwort-Manager
  - Fragen ?

Passwort-Sicherheit

Länge oder Anzahl differierende Zeichen ?

- 4-stelliges Passwort,
  26 zur Verfügung stehende Zeichen (a-z)

- Formel: $C_{max} = n_c^{l}$
  - C_{max} = Anzahl mögliche Kombinationen von Passwörtern
  - ^{l} = Passwortlänge
  - n_c = Zeichenvorrat (Anzahl differenter Zeichen)

- $C_{max} = n_c^{I} = 26^4 = 456'976$ Kombinationen

Passwort-Sicherheit

Länge oder Anzahl differierende Zeichen ?

- $C_{max} = n_c^l = 26^4 = 456'976$ Kombinationen
- Wir erhöhen nun die Länge $l = l + 1$ und $n_c = n_c + 1$
- $C_{max} = 27^4 = 531'441$ Kombinationen
- $C_{max} = 26^5 = 11'881'376$ Kombinationen
- Fazit: → Länge vor Varianz !

Passwort-Sicherheit

- ***Agenda***
  - Warum brauche ich ein sicheres Passwort ?
  - Was ist ein sicheres Passwort ?
  - Länge oder Anzahl differierender Zeichen
  - Passwort-Manager
  - Fragen ?

Passwort-Sicherheit

Passwort-Manager ?

- Ich benötige möglichst lange Passwörter
- Eines pro Account / Webdienst
- Mit Sonderzeichen, möglichst kryptisch (keine bekannten Worte)
- Wie soll ich die alle behalten ?
  →Mögliche Lösungsansätze:
  1. Kombination aus sicherem Mittelteil und Webseite (s. Folie 12 weiter vorne)
  2. Passwort-Manager

Passwort-Sicherheit

Passwort-Manager

- Ein Passwort-Manager ermöglicht mir das Speichern meiner Passworte in einem Container
- Ich muss mir noch genau ein Master-Passwort merken
- Alle anderen Passwörter sind im Container und können beliebig lange, kompliziert, unleserlich und unabtippbar sein
- Ich muss mir Gedanken über die Verfügbarkeit und (u.U. auch zur Aktualität) meines Containers auf verschiedenen Systemen (Desktop, Laptop, Tablet, Smartphone) machen
- Bitte nicht den PW-Container des Browsers verwenden !!!

Passwort-Sicherheit

Passwort-Manager – Übersicht

Kriterium	Lastpass	1Password	Keepass	Dashlane	Enpass
Linux	X	-	X	-	X
Windows	X	X	X	X	X
Mac	X	X	X	X	X
Android	X	X	X	X	X
iOS	X	X	(X)	X	X
Preis	125 $ p.a.	36 $ p.a. (1 User) 60 $ p.a. (5)		0 $ (1 Gerät) 40 $ p.a. (n)	10 $ pro Betriebssystem
2FA	Ja	Nein	Nein	Ja	Nein
Sprachen	D / F / E	D / E	D / E / F	E / F / D / I / S / P	E
Formular-assistent	Ja	Ja	Nein	Ja	Ja
Daten gespeichert	Cloud	Cloud	Lokale Datei	Cloud	Lokale Datei, optional Cloud
Sync	Via Cloud	Via Cloud	Manuell – Import File	Automatisiert möglich	Via Cloud

Links und Infos I

- Kaspersky Lab - Secure PW Check
- Christian Bossert - Passwort Sicherheit
- David Blum - Der Schlüssel zur sicheren PW-Strategie
- Der Sicherheits-Blog für den Mittelstand

Fragen ?

Jederzeit auch via Mail:

daniel.haenni@sbb.ch

Input aus Diskussion BLUG

- Vorschlag mit Web-Dienst vorne und hinten und sicherem Mittelteil ist noch zu wenig sicher, wenn jemand den Mittelteil in Erfahrung bringt, ist es für ihn ein einfaches, den Mechano mit Webdienst vorne und hinten zu erkennen und so diverse Web-Dienste durchzuprobieren.
- Webdienst vorne / hinten auch noch anonymisieren, Amazon = Amazönli, Facebook = Gsichtsbuech
- Vorschlag: keine Sonderzeichen, keine y, z, keine Umlaute, 4 deutsche Worte aneinander gereiht, die nichts miteinander zu tun haben (Beispiel: Wagenburg-Solothurn-Sonne-Gestern).