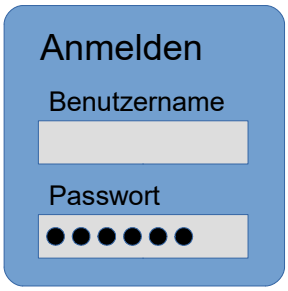


Schutz im Internet über ein sicheres Passwort

J. Diefenbach
PC-Lernwerkstatt Ehningen
pc-lernwerkstatt@gemeinde-ehningen.de

Inhaltsverzeichnis

- Einführung
- Methoden, Passwörter zu stehlen
- Knacken gehashter Passwörter
- Erstellen eines sicheren Passworts
- Sicherer Umgang mit Passwörtern
- Zugang mit erhöhter Sicherheit
- Zusammenfassung
- Quellen

Inhaltsverzeichnis

- Einführung
- Methoden, Passwörter zu stehlen
- Knacken gehashter Passwörter
- Erstellen eines sicheren Passworts
- Sicherer Umgang mit Passwörtern
- Zugang mit erhöhter Sicherheit
- Zusammenfassung
- Quellen

Einführung

Datenklau

Januar 2019

SPIEGEL ONLINE
04. Januar 2019, 08:14 Uhr

Datenklau

Hackerangriff auf Hunderte deutsche Politiker

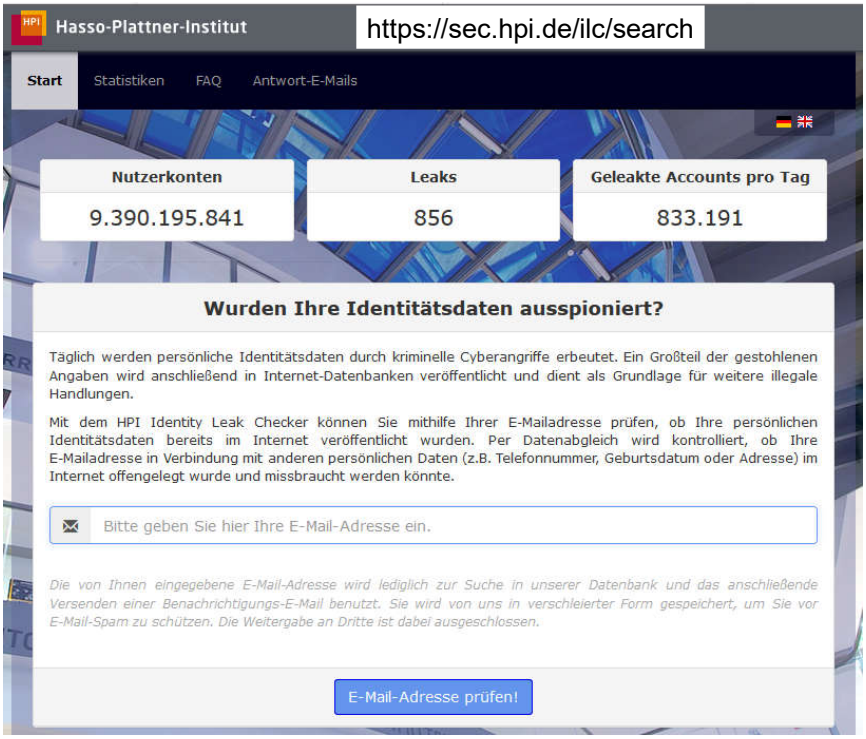
Handynummern, Adressen, Briefe und Kreditkarteninfos: Hacker haben auf Twitter massenweise Daten deutscher Politiker veröffentlicht. Wer hinter dem Angriff steckt, ist noch unklar.

Politiker im Bundestag und aus den Ländern sind Opfer eines Hackerangriffs geworden. Unbekannte haben massenweise Daten und Dokumente im Internet veröffentlicht. Betroffen sind vor allem im Bundestag vertretenen Parteien - nur nicht die AfD.

Wer dafür verantwortlich ist und welche Motivation dahintersteckt, ist noch unklar. Auch ob alle Daten authentisch sind, war zunächst offen. Zunächst hatte das rbb-Inforadio darüber berichtet.

Die Hacker verschafften sich offenbar Zugriff auf Kontaktdaten wie Handynummern und Adressen der Politiker, aber auch auf parteiinterne Dokumente und persönliche Daten. Darunter sind auch Bilder von Personalausweisen, Briefe, Rechnungen, Einzugsermächtigungen oder Kreditkarteninformationen aus dem Familienkreis. Zum Teil sind die Daten mehrere Jahre alt.

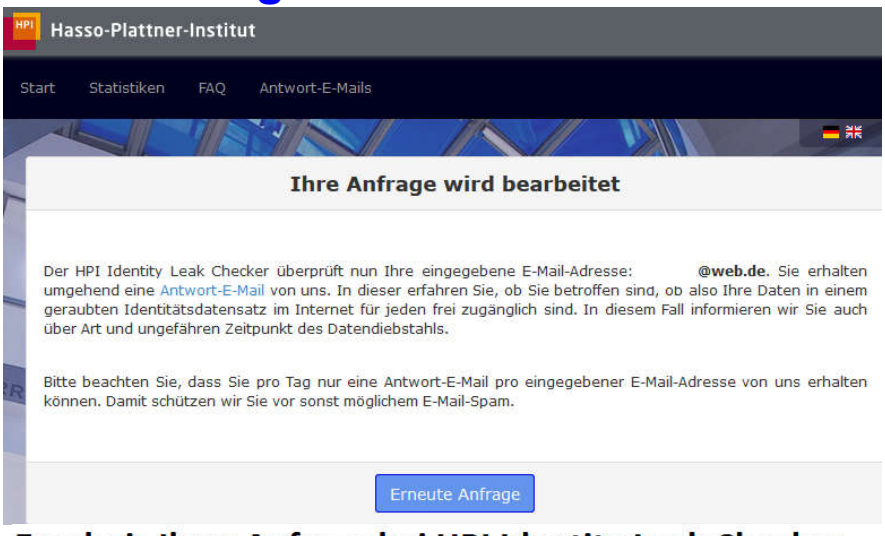
Mit Email-Adresse und Passwort konnte ein Hacker persönliche Daten abgreifen



Prüfen, ob das Konto gehackt ist

Datum 22.4.2019

Einführung



Konto nicht gehackt

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Glückwunsch: Ihre E-Mail-Adresse @web.de taucht nicht in unserer Datenbank auf. Das garantiert jedoch nicht, dass keine Ihrer persönlichen Informationen gestohlen wurden.

Einführung

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse max.mustermann@domain.de taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf.
Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozialversicherungsnr.	IP-Adresse
Leak A	Apr. 2016	✓	Betroffen	-	Betroffen	-	-	-	Betroffen	-	-
Leak B	Mär. 2014		Betroffen	-	-	Betroffen	Betroffen	Betroffen	-	-	-

Betroffen: Diese Daten wurden in der zum angegebenen Zeitpunkt veröffentlichten Identitätsdatenbank der jeweiligen Quelle gefunden.
-: Es wurden keine solche Daten gefunden.

Bei einem *verifizierten* Leak (dargestellt mit ✓) handelt es sich um ein vom Dienstbetreiber bestätigtes Datenleck bzw. das Vorliegen eines Datenlecks beim Dienst ist hochwahrscheinlich. Bei einem *nicht verifizierten* Leak (fehlendes ✓) ist die Herkunft der Daten und deren Legitimät ungewiss. Solche unverifizierten Daten könnten z.B. aus Sammlungen von Passwörtern oder Kombinationen mehrerer älterer Leaks stammen oder auch generiert sein. Das Vorkommen in einem solchen Leak ist demnach kein sicherer Indikator für ein Datenleck.

Bitte beachten Sie, dass wir aus Sicherheitsgründen keine Auskunft über die konkret betroffenen Daten in den aufgeführten Kategorien geben können.

Wir empfehlen die folgende Reaktion:

- **Passwort:** Ändern Sie Ihr Passwort für sämtliche Accounts mit der E-Mail-Adresse max.mustermann@domain.de, bei denen das Passwort älter oder gleich dem angegebenen Datum ist.
- **Kreditkartendaten:** Informieren Sie umgehend Ihre Banken über den Diebstahl und sperren Sie ihre betroffenen Kreditkarten. Halten Sie Ausschau nach verdächtigen Transaktionen, die über Ihre Kreditkarten getätigt werden.
- **Bankkontodaten:** Informieren Sie umgehend Ihre Banken über den Diebstahl. Halten Sie Ausschau nach verdächtigen Transaktionen, die über Ihr Bankkonto getätigt werden.
- **Telefonnummer:** Ändern Sie bei belästigenden Anrufen gegebenenfalls Ihre Telefonnummer. Achten Sie auf betrügerische Anrufe, die sich die von Ihnen gestohlene Identität zu Nutze machen.

Generell gilt, dass je mehr Identitätsdaten über Sie veröffentlicht werden, desto leichter kann Ihre Identität missbraucht werden.
Es ist auf jeden Fall ratsam eine Anzeige beim Diebstahl von Informationen wie Bankdaten, Kreditkartendaten und Sozialversicherungsnummern zu erstatten.

Haftungsausschluss: *Wir übernehmen keine Haftung für die Vollständigkeit und Korrektheit der bereitgestellten Informationen unseres Dienstes. Die Daten werden automatisch gesammelt und entsprechend für Abfragen aufbereitet. Wir werten für unseren Dienst nur öffentlich im Internet verfügbare Quellen aus und können keine Vollständigkeit garantieren. Wir bereiten nur den Teil der im Internet veröffentlichten Identitätsdatenbanken auf und haben keinen Zugriff auf "analoge Daten", also z.B. Daten, die physikalisch von Betrügern ausgetauscht werden oder Daten die von Dokumenten (Reisepass, Ausweis, Rechnungen, persönliche Briefe) abgeschrieben werden.*

Ihr HPI Identity Leak Checker Team
Webseite

Konto wurde gehackt

Einführung

Welche Motivation haben Kriminelle?

1. Geld

2. Ausspähen des Opfers und Bloßstellung (Doxing)

3. Spionage
   - Wirtschaftsspionage: Betriebsgeheimnisse
   - Angriffe auf Infrastruktur

Einführung

Das Internet wird immer mehr für sensible Transaktionen genutzt

- Verträge werden online abgeschlossen (Kaufverträge, Reisen,…..)
- Online-Kommunikation (email, Messenger, ...)

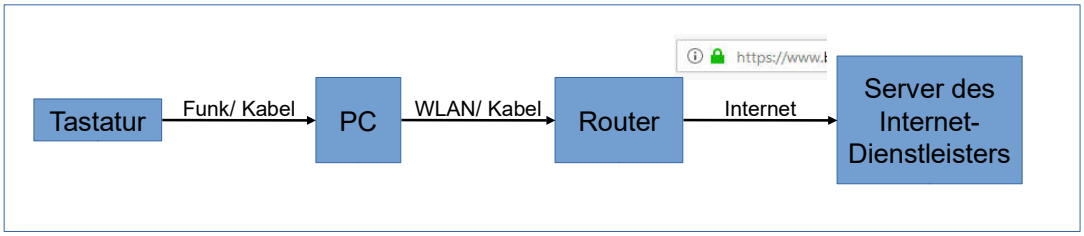
Facebook,
Twitter
WhatsApp

- Online-Banking (Überweisungen, Depotverwaltung)

Notwendigkeit zum Nachweis der Identität des Benutzers

Einführung

Wie funktioniert eine Identifikation über Passwort?



1) Der Nutzer tippt das Passwort auf der Tastatur ein.
2) Über das Internet wird das Passwort zum Server des Internet-Dienstleisters übertragen.
3) Der Server prüft das Passwort.
4) Ist das Passwort korrekt, erlaubt der Server den Zugang.

Auf dem Server ist das Passwort gespeichert.

Einführung

Auch ohne Passwort kann man Zugang erhalten

Der berechtigte Nutzer hat das Passwort vergessen:

1. Internetdienstleister sendet Ersatzpasswort an Email-Adresse	z. B. Amazon, Deutsche Bahn
2. Internetdienstleister sendet Ersatzpasswort über SMS an Telefonnummer (Handy/ Smartphone)	z. B. web.de
3. Nutzer antwortet auf „Sicherheitsfrage“ (Antwort wurde bei Anmeldung hinterlegt)	- Geburtsname der Mutter - Lieblingsfarbe etc.

Inhaltsverzeichnis

- Einführung
- Methoden, Passwörter zu stehlen
- Knacken gehashter Passwörter
- Erstellen eines sicheren Passworts
- Sicherer Umgang mit Passwörtern
- Kein Zugang zum eigenen Konto
- Zusammenfassung
- Quellen

Methoden, Passwörter zu stehlen

Im unmittelbaren Umfeld

- Zettel mit Passwort öffentlich sichtbar

z. B. auf dem Bildschirm
oder unter der Tastatur

Methoden, Passwörter zu stehlen

Im unmittelbaren Umfeld

Menschen im unmittelbaren Umfeld bekommen Einblick auf das Passwort

- „Blick über die Schulter“ beim Eintippen

z. B. in öffentlichen Verkehrsmitteln

- Passwort lässt sich erraten

Geburtsdatum,
Vorname des Kindes

- Passwort ist im Browser gespeichert

- Im Browser gespeicherte Passwörter kann jeder verwenden, der das Gerät bedient.
- Passwörter werden im Klartext gespeichert

- Belauschen des Verkehrs einer Funktastatur
- Belauschen des Verkehrs eines offenen WLANs

Methoden, Passwörter zu stehlen

Aus der Entfernung

- „Social Engineering“:
  Versuche, über direkte Kontakte das Vertrauen und dann das Passwort zu erhalten.

Polizeibericht aus Leonberg

Frau lässt Trickbetrüger abblitzen

Von Henning Maak - 20. Januar 2018 - 18:00 Uhr

Angeblicher Microsoft-Mitarbeiter will Zugang zu ihrem Computer.

https://www.stuttgarter-zeitung.de/inhalt.polizeibericht-aus-leonberg-frau-laesst-trickbetrueger-abblitzen.e6b6fa3e-d3fc-4504-a20b-5497265d0547.html

- Schadsoftware (Keylogger) auf PC/Smartphone protokolliert Eingaben auf der Tastatur und sendet sie über das Internet.

z.B. durch Anklicken eines Anhangs einer email

- Bei unverschlüsselter Übertragung kann das Passwort auf dem Weg vom PC/Smartphone zum Internet-Dienstleister abgefangen werden.

Methoden, Passwörter zu stehlen

Aus der Entfernung

- Phishing-emails

Postfach

Betreff	Beteiligte	Datum
Bestätigung ihres Amazon-Kontos nötig	Amazon.de	19.11.2018, 18:28

Methoden, Passwörter zu stehlen

Phishing-emails

Amazon

Guten Tag,

nach der neuen EU-Datenschutzverordnung sind wir zur regelmäßigen Identitätskontrolle verpflichtet.

Laut Grundverordnung ist dieser Schritt notwendig, um das Vertrauen der Verbraucher beim Bezahlen im Internet und damit den Online-Handel an sich zu stärken.

Ihre Identität wird dann automatisch von unserem Sicherheitssystem geprüft. Klicken Sie auf die unten stehende Fläche, um die Überprüfung zu beginnen.

Identität prüfen

Mit freundlichen Grüßen,
Amazon Kundendienst

Mit dieser Servicemitteilung informieren wir Sie über wichtige Änderungen bezüglich Ihres Amazon Kontos.
Copyright © 1998-2018 Amazon.com. Alle Rechte vorbehalten.

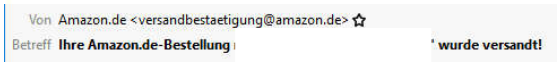
- Über einen Link in der email gelangt man auf eine gefälschte Webseite.

Dort soll man das Passwort eingeben.

Methoden, Passwörter zu stehlen

Phishing-emails

gefälscht



echt

Vorsicht
- bei unbekannten Absendern
- bei Abfragen von Passwort, etc.

Gegenmaßnahmen
+ Webseite immer über den Browser ansteuern
+ Nachforschen beim wahren Internetdienst
+ Wenn man den Absender googelt, findet man Warnungen

Niemals Link in email anklicken oder Anhang öffnen

Methoden, Passwörter zu stehlen

Passwortklau beim Internet- Dienstleister

SPIEGEL ONLINE
04. Oktober 2017, 03:19 Uhr

Hackerangriff von 2013

Alle drei Milliarden Yahoo-Accounts betroffen

Internet-Dienstleister speichern das Passwort verschlüsselt als sogenannter „Hash“.

Bei der Anmeldung berechnet der Server den Hash des Passwortes und vergleicht mit dem abgespeicherten Hash.

Sicherheit:
Der Hash wird aus dem Passwort berechnet, das Passwort aber nicht aus dem Hash.

Der Hacker muss den Hash knacken, um den Zugang mit dem Passwort zu erhalten.

Inhaltsverzeichnis

- Einführung
- Methoden, Passwörter zu stehlen
- Knacken gehashter Passwörter
- Erstellen eines sicheren Passworts
- Sicherer Umgang mit Passwörtern
- Zugang mit erhöhter Sicherheit
- Zusammenfassung
- Quellen

Knacken gehashter Passwörter

1. Angriff mit „Roher Gewalt“ (Brute Force Attack)

Erbeutete Passwort-Hashes können offline entschlüsselt werden.
Die mathematische Funktion lässt sich nicht umkehren.

Man berechnet den Hash
für „alle“ Zeichen-Kombinationen

Klartext	Hash (MD5)
passwort	5f4dcc3b5aa765d61d8327deb882cf99
passwort1	64397c8527190222aa6d61b3c23f8e84

Für Verschlüsselungsfunktionen
(hier MD5) sind Tabellen im Internet
zu finden („rainbow table“).

Art /Anzahl Zeichen		Wortlänge
Kleinbuchst./Ziffern	36	1 bis 9
Groß-/Kleinbuchst./Ziffern	62	1 bis 9
Groß-/Kleinbuchst./Ziffern, Sonderzeichen	95	1 bis 8

Knacken gehashter Passwörter

Stärke = Zeit, in der es entschlüsselt werden kann
= Anzahl der möglichen Passwörter

2 Faktoren bestimmen die Stärke eines Passworts (E)
- Z: Anzahl der möglichen Zeichen des Zeichensatzes
- L: Länge des Passworts

$$E = L * \log(Z)/\log(2)$$

Name des Zeichensatzes	Zeichen	Zeichensatz
Ziffern	10	0 1 2 3 4 5 6 7 8 9
Kleinbuchstaben	26	a b c d e f g h i j k l m n o p q r s t u v w x y z
Großbuchstaben	26	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Sonderzeichen der amerikan. Tastatur	32	! “ # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
Leerzeichen	1	

Gilt nur, wenn jedes Zeichen zufällig gewählt wird!!!

Knacken gehashter Passwörter

Beispiele der Stärke von zufälligen Passwörtern

Länge	Zeichensatz	Anzahl der Möglichkeiten	
10	Nur Ziffern (10*10* … *10)	10^{10}	
14	Nur Ziffern	10^{14}	
10	Kleinbuchstaben	$26^{10} = 1{,}4\ 10^{14}$	
14	Kleinbuchstaben	$26^{14} = 6{,}4\ 10^{19}$	
10	Groß-/Kleinbuchst., Ziffern	$62^{10} = 8{,}4\ 10^{17}$	
14	Groß-/Kleinbuchst., Ziffern	$62^{14} = 6{,}1\ 10^{21}$	
10	Groß-/Kleinbuchst., Ziffern, Sonderzeichen, Leerzeichen	$95^{10} = 6{,}0\ 10^{19}$	
14	Groß-/Kleinbuchst., Ziffern, Sonderzeichen, Leerzeichen	$95^{14} = 4{,}9\ 10^{27}$	

Knacken gehashter Passwörter

Beispiele der Stärke von zufälligen Passwörtern

Länge	Zeichensatz	Anzahl der Möglichkeiten	Stärke
10	Nur Ziffern (10*10* … *10)	10^{10}	33
14	Nur Ziffern	10^{14}	47
10	Kleinbuchstaben	$26^{10} = 1{,}4\ 10^{14}$	47
14	Kleinbuchstaben	$26^{14} = 6{,}4\ 10^{19}$	66
10	Groß-/Kleinbuchst., Ziffern	$62^{10} = 8{,}4\ 10^{17}$	60
14	Groß-/Kleinbuchst., Ziffern	$62^{14} = 6{,}1\ 10^{21}$	83
10	Groß-/Kleinbuchst., Ziffern, Sonderzeichen, Leerzeichen	$95^{10} = 6{,}0\ 10^{19}$	66
14	Groß-/Kleinbuchst., Ziffern, Sonderzeichen, Leerzeichen	$95^{14} = 4{,}9\ 10^{27}$	92

Knacken gehashter Passwörter

Anlage zum Knacken eines Passworts

testet 327 Mrd. Schlüssel pro Sekunde (0,3 *10^{12})

gebaut aus Standard-PC-Komponenten (2017):

- Intel i7-6800K Prozessor
- 64 GB RAM
- 4 Graphik-Karten Nvidia GTX 1080TI

kombiniert mit älterer Maschine

Preis: $ 5110

https://www.blackhillsinfosec.com/build-password-cracker-nvidia-gtx-1080ti-gtx-1070/

Knacken gehashter Passwörter

Beispiele der Stärke von zufälligen Passwörtern

Länge	Zeichensatz	Anzahl der Möglichkeiten	Zeit bis zum Knacken
10	Nur Ziffern (10*10* … *10)	10^{10}	0,03 sec
14	Nur Ziffern	10^{14}	5,1 Minuten
10	Kleinbuchstaben	$26^{10} = 1{,}4\ 10^{14}$	7,2 Minuten
14	Kleinbuchstaben	$26^{14} = 6{,}4\ 10^{19}$	6,3 Jahre
10	Groß-/Kleinbuchst., Ziffern	$62^{10} = 8{,}4\ 10^{17}$	9,7 Tage
14	Groß-/Kleinbuchst., Ziffern	$62^{14} = 1{,}2\ 10^{25}$	1,2 Mio. Jahre
10	Groß-/Kleinbuchst., Ziffern, Sonderzeichen, Leerzeichen	$95^{10} = 6{,}0\ 10^{19}$	5,8 Jahre
14	Groß-/Kleinbuchst., Ziffern, Sonderzeichen, Leerzeichen	$95^{14} = 4{,}9\ 10^{27}$	473 Mio. Jahre

Knacken gehashter Passwörter

Analyse tatsächlicher Passwörter

Die Wahrscheinlichkeit des Auftretens der einzelnen Zeichen ist unterschiedlich!

1. Zahlen: Die Wahrscheinlichkeit der Zahl 1 ist höher als die der anderen Zahlen
2. Buchstaben: Die häufigsten Buchstaben sind a, e, o, r

Die Wahrscheinlichkeit des „e“ ist 6mal höher als die des „f“.

3. Sonderzeichen (amerikanische Tastatur):

   ! “ # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

   deutlich geringere Wahrscheinlichkeit als Buchstaben

https://en.wikipedia.org/wiki/Password_strength

Selbst ausgedachte Passwörter haben eine wesentlich höhere Wahrscheinlichkeit als zufällig von einem Algorithmus errechnete.

Knacken gehashter Passwörter

2. Wörterbuch Angriff (Dictionary Attack)

Man probiert:

- Wörter aus Wörterbuch,
- Markennamen,
- Zitate
- erbeutete Passwörter aus bisherigen Hacks

Mit Anhang 1, !, 01, etc.

Bekanntes Ersetzen von Buchstaben durch Sonderzeichen
A durch @
O durch 0
S durch 5

Neue Passwort-Leaks: Insgesamt 2,2 Milliarden Accounts betroffen

25.01.2019 12:51 Uhr
Ronald Eikenberg

https://www.heise.de/security/meldung/Neue-Passwort-Leaks-Insgesamt-2-2-Milliarden-Accounts-betroffen-4287538.html

Inhaltsverzeichnis

- Einführung
- Methoden, Passwörter zu stehlen
- Knacken gehashter Passwörter
- Erstellen eines sicheren Passworts
- Sicherer Umgang mit Passwörtern
- Zugang mit erhöhter Sicherheit
- Zusammenfassung
- Quellen

Erstellen eines sicheren Passworts 1/9

Vorüberlegungen

Welcher Schaden kann mir entstehen,
wenn das Passwort in falsche Hände gerät?

Besonders schützen:
- email-Adresse
- Online-Bank
- soziales Netzwerk

Die email-Adresse wird von Internet-Dienstleistern genutzt, um Zugang zu ermöglichen, wenn man sein Passwort vergessen hat

Bei vielen Internet-Dienstleistern kann man sich über Facebook einloggen.

Die folgenden Empfehlungen gelten für Anwendungen,
die stark geschützt werden müssen.

Erstellen eines sicheren Passworts 2/9

Anforderungen an ein Passwort

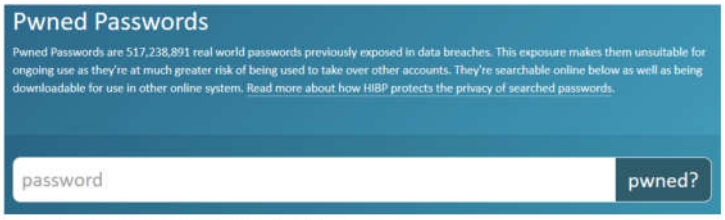
- Sicher: nur in sehr langer Zeit zu knacken

- Leicht zu merken

Erstellen eines sicheren Passworts 3/9

Regeln

1. Länge: mindestens 10 Zeichen (je länger, desto sicherer)
2. Kein Wort verwenden, das in einem Wörterbuch steht
3. Kein Passwort verwenden, das bereits geknackt worden ist



Enthält 517,238,891 Worte

https://haveibeenpwned.com/Passwords

Internetdienstleister soll das Passwort bei der Anmeldung mit einer Liste geknackter Passwörter (Blacklist) abgleichen

Nachtrag 17.1.2019
551,509,767 Worte

Erstellen eines sicheren Passworts 5/9

Methode1 1/2

Erstellen eines Passworts mit dem Passwortmanager Keepass Open Source

erzeugt über
Tools → Password Generator
ein zufälliges Passwort

Erstellen eines sicheren Passworts 6/9

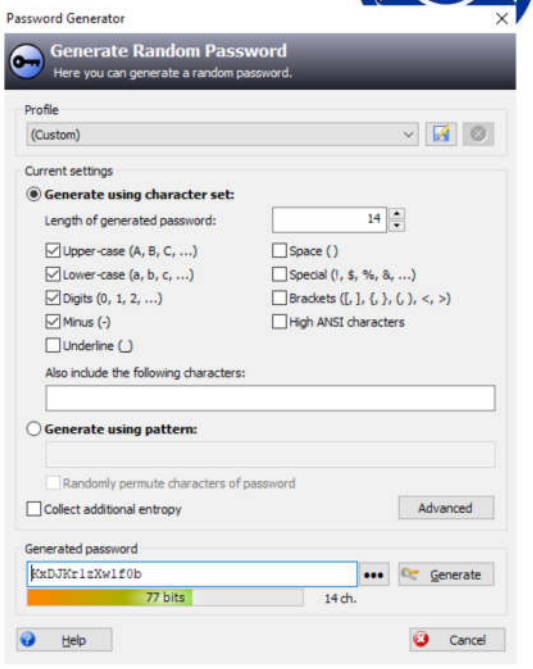
Methode1 2/2

Passwortmanager Keepass

26+26+10+1 Zeichen bei 14 Stellen
1,55* 10^{25} Möglichkeiten

Stärke E = 77 Bit

Bei 327 Mrd. Schlüsseln /sec
geknackt in 1,5 Mio. Jahren



Erstellen eines sicheren Passworts 7/9

Methode2: Diceware 1/2

Dice = Würfel

Idee:
Erzeugen eines Passwortes aus zufälligen Wörtern

Correct Horse Battery Staple

Würfeln auf Basis einer Tabelle mit 7776 Einträgen

5 Würfe mit einem Würfel ergeben 6 * 6 * 6 * 6 * 6 = 7776 Möglichkeiten

11554	2015	12131	:-)	12264	abrupt
11555	2020	12132	;	12265	abs
11556	2030	12133	?	12266	absage
11561	2035	12134	??	12311	absatz
11562	2040	12135	???	12312	abschn
11563	2045	12136	@	12313	absenz
11564	2050	12141	+	12314	absurd
11565	2222	12142	++	12315	abt
11566	2345	12143	+++	12316	abtei
11611	2468	12144	=	12321	abteil
11612	3000	12145	==	12322	abtun
11613	3333	12146	===	12323	abu
11614	3456	12151	a	12324	abuja
11615	4000	12152	aa	12325	abweg

http://world.std.com/~reinhold/diceware.html

Erstellen eines sicheren Passworts 8/9

Methode2: Diceware 2/2

Vorgehensweise:

1. 5 Würfe ergeben eine Zahlenfolge
   Dazu gehört ein Wort aus der Tabelle als erster Teil des Passworts
2. Man wiederholt dies weitere 4 Mal
3. Man erhält ein leicht zu merkendes Passwort aus 5 Worten

z. B. 51666 ergibt das Wort raspel

Stärke: E = 65 Bit $E = 5 * \log(7776)/\log(2)$

Bei 327 Mrd. Schlüsseln /sec
geknackt in 2,75 Jahren

z. B. raspel wermut keule pkt mobil
Hier 25 Zeichen lang

7776 * 7776 * 7776 * 7776 * 7776 = 2,8 * 10^{19} Möglichkeiten

Erstellen eines sicheren Passworts 9/9

Methode3: Passphrase

1. Basis ist ein einfach zu merkender Satz
   my cat's paw is red and sore (Die Pfote meiner Katze ist rot und entzündet)
2. Entferne die Leerzeichen und schreibe den Anfangsbuchstaben des zweiten Wortes groß
   myCat'spawisredandsore (22 Zeichen bei 52 Zeichen: 125 Bit)
3. Ändere die a's in @ und die s's in $
   myC@t'sp@wi$red@nd$ore

Ein leicht zu merkendes Passwort mit 22 Zeichen (Zeichensatz 54 Zeichen)

Stärke: E = 126 Bit (1,3 10^{38} Kombinationen)

Bei 327 Mrd. Schlüsseln /sec geknackt in 6* 10^{18} Jahren

https://www.ricksdailytips.com/create-secure-password/

Inhaltsverzeichnis

- Einführung
- Methoden, Passwörter zu stehlen
- Knacken gehashter Passwörter
- Erstellen eines sicheren Passworts
- Sicherer Umgang mit Passwörtern
- Zugang mit erhöhter Sicherheit
- Zusammenfassung
- Quellen

Sicherer Umgang mit Passwörtern 1/3

Regeln für Umgang mit Passwörtern

1. Für jede Anwendung ein eigenes Passwort
2. Voreingestellte Passwörter ändern
3. Passwort nur ändern, wenn der Verdacht besteht, dass es unsicher ist
4. Keine Sicherheitsfragen verwenden
5. Programme aktuell halten, Antiviren-Software verwenden
6. Passwörter nur auf vertrauenswürdigen Rechnern eingeben

Ansonsten muss man nach einem Hack eines Internet-Dienstes alle Passwörter ändern!

Antworten werden bei Passwort-klau oft im Klartext abgegriffen

Schutz vor Viren/ Trojanern

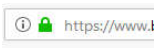
Vorsicht: beim Passwortmanager Keepass wurde über angebliches Updates Schadsoftware aufgespielt

Sicherer Umgang mit Passwörtern 2/3

Regeln für Umgang mit Passwörtern

7. Passwort nicht im Browser/ Email-Programm speichern
8. Eingabe von Passwörtern nur über verschlüsselte Internetverbindung
9. Keine Passwörter in offenem WLAN eingeben
10. Verdächtige emails: nicht auf Links klicken oder Anhänge öffnen, auf gar keinen Fall Passwörter/ TAN eingeben.
11. Vorsicht bei Telefonanrufen angeblicher Microsoft
12. Haben Erben Zugriff auf die Passwörter?
13. 2-Faktor-Autorisierung nutzen

Firefox, Chrome, Thunderbird, etc.



Phishing

Passwörter aufschreiben und an einem sicheren Ort lagern

Sicherer Umgang mit Passwörtern 3/3

Passwortmanager

Keepass	kostenlos	
Lastpass	ca. 19,50 €	Test in c't 7/2018

Risiko:

1. Wenn der Passwort-Tresor geknackt wird, liegen alle Passwörter offen
2. Passwortmanager sind bevorzugtes Ziel von Hacker-Angriffen

Hackertool KeeFarce stiehlt in Keypass gespeicherte Passwörter

https://www.ricksdailytips.com/keefarce/#more-27729

Inhaltsverzeichnis

- Einführung
- Stärke eines Passwortes
- Methoden, Passwörter zu stehlen
- Knacken gehashter Passwörter
- Sicherer Umgang mit Passwörtern
- Zugang mit erhöhter Sicherheit
- Zusammenfassung
- Quellen

Nachweis der Identität

Geldautomat (2-Faktor-Identifizierung)

Identifikation über 2 unabhängige Elemente

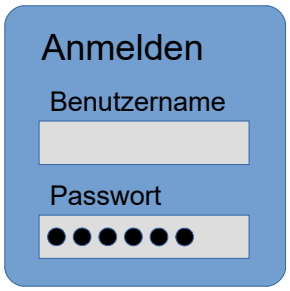
1. Karte — Besitz
2. Geheimzahl (PIN) — Wissen

Bild aus de.wikipedia.org

Internet (übliches Verfahren)

Identifikation über

- User Name — Wissen
- Passwort — Wissen

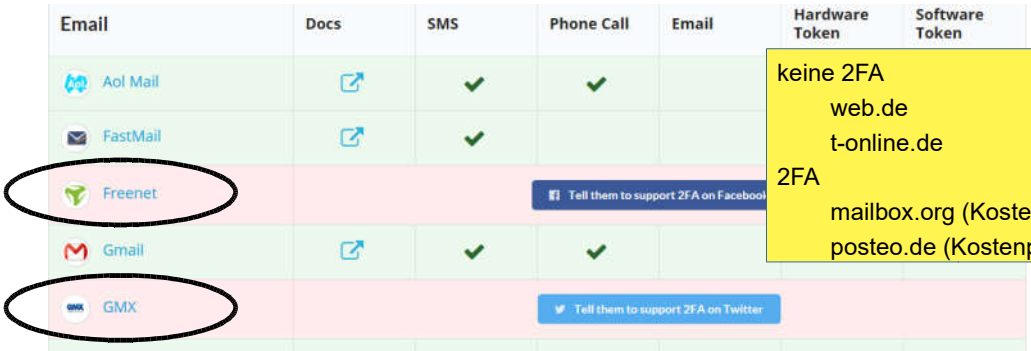


Alternativen zum Passwort
- Biometrische Kennzeichen (z. B. Fingerabdruck-Scan, Gesicht)
- Wischmuster (Smartphone)

Einführung
Zugang mit erhöhter Sicherheit

2-Faktor-Autorisierung (2FA)

Welche Internetdienstleister 2-Faktor-Autorisierung anbieten, kann man auf https://twofactorauth.org abfragen:



keine 2FA
- web.de
- t-online.de

2FA
- mailbox.org (Kostenpflichtig)
- posteo.de (Kostenpflichtig)

Einführung
Zugang mit erhöhter Sicherheit

2-Faktor-Autorisierung (2FA)	Keine 2-Faktor-Autorisierung
amazon	Deutsche Bahn
Apple	Lufthansa
ebay	IKEA
facebook	Zalando
instagram	
twitter	
xing	

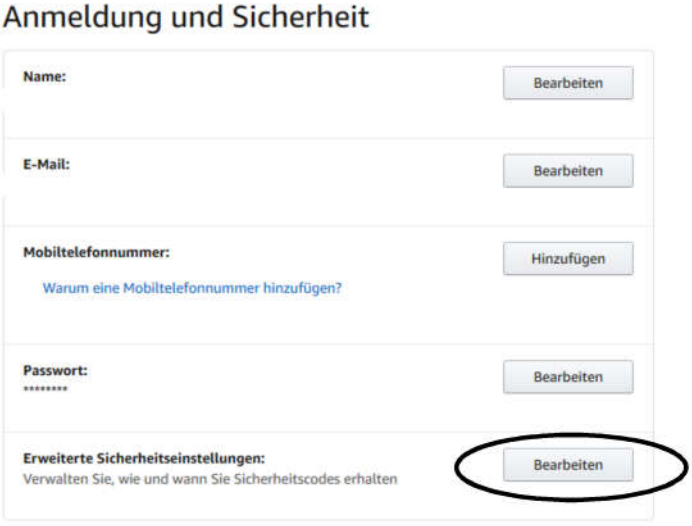
Einführung
Zugang mit erhöhter Sicherheit

Einrichten der 2-Faktor-Autorisierung bei amazon.de

Passwort — Wissen
Smartphone — Besitz

Aktivierung der 2FA

- Konto
- Anmeldung und Sicherheit
- Erweiterte Sicherheits-einstellungen



Einführung
Zugang mit erhöhter Sicherheit

Einloggen mit 2-Faktor-Autorisierung bei amazon.de

Wie funktioniert es?

Nachdem Sie die Zwei-Schritt-Verifizierung für Ihr Konto aktiviert haben, verläuft die Anmeldung wie folgt:

1. Sie geben wie gewohnt Ihr Passwort ein.
2. Wir senden Ihnen einen Code an Ihr Mobiltelefon.
3. Sie geben den Code ein und schließen Ihre Anmeldung ab.

Man kann bestimmte Geräte von der 2FA ausnehmen, bei denen der Missbrauch unwahrscheinlich ist (z. B. PC in der eigenen Wohnung).

Kein Zugang zum eigenen Konto

Mögliche Ursachen

1. Fehler bei der Eingabe von Kontoname oder Passwort
   z. B. Feststelltaste/Num-Taste korrekt eingestellt, Siehe LEDs auf der Tastatur
   z. B. falsches Zeichen/Passwort eingegeben
2. falsche Spracheinstellung (z.B. englische Tastatur)
3. keine Verbindung mit Internet
4. bei 2-Faktor-Autorisierung: Code überprüfen

Inhaltsverzeichnis

- Einführung
- Methoden, Passwörter zu stehlen
- Knacken gehashter Passwörter
- Erstellen eines sicheren Passworts
- Sicherer Umgang mit Passwörtern
- Zugang mit erhöhter Sicherheit
- Zusammenfassung
- Quellen

Zusammenfassung

Schutz der digitalen Identität

1. Nutzen von 2-Faktor Autorisierung, wenn möglich

2. Erzeugen eines starken Passwortes
   mit einem Passwort-Manager

ODER

   über Diceware

ODER

   Passphrase

Inhaltsverzeichnis

- Einführung
- Methoden, Passwörter zu stehlen
- Knacken gehashter Passwörter
- Erstellen eines sicheren Passworts
- Sicherer Umgang mit Passwörtern
- Zugang mit erhöhter Sicherheit
- Zusammenfassung
- Quellen

Weitere Quellen

/1/ c't-Magazin 7/2018

/2 /: Übersicht über Verschlüsselungsmethoden

https://ehash.iaik.tugraz.at/wiki/The_Hash_Function_Zoo

/3 / https://www.bsi-fuer-buerger.de/

/4 / https://twofactorauth.org

/5 / rainbow table nach http://project-rainbowcrack.com

/6 / Mike Kuketz: https://www.kuketz-blog.de/