Die Passwörter der Hacker

02. Mai 2016 - Von Simon Hülsbömer (Leitender Redakteur) CIO

Dass sich Nutzer keine Passwörter merken können und nur wenige einen Passwort-Manager einsetzen, machen sich Hacker zunutze: Viele Systeme knacken sie ganz einfach durch Eingabe von Standard-Codes. Wir stellen die am häufigsten verwendeten Hacker-Passwörter vor.

Die Security-Analysten von Rapid7 haben das "Hacker's Dictionary" veröffentlicht - eine Aufstellung der am häufigsten durch Hacker "bei der Arbeit" verwendeten Nutzername/Passwort-Kombinationen. Zusammengestellt werden konnten die Listen dank des öffentlich zugänglichen Honeypot-Netzes von Rapid7 namens "Heisenberg", mit dem Hacker fast ein Jahr lang dazu gebracht werden konnten, Eindringversuche in Fake-Systeme zu unternehmen.

Es sind zumeist keine Menschen, die diese Login-Versuche unternehmen, sondern von ihnen entwickelte automatisierte Scanroutinen, die mit dem Internet verbundene Systeme und Dienste auf Schwachstellen prüfen und unterwandern sollen. Deshalb gibt das "Hacker's Dictionary" einen ziemlich guten Aufschluss über die dort verwendeten Standard-Kombinationen aus Nutzernamen und Passwörtern. Betroffen sind Point of Sale (POS)-Systeme, Kioske und durch Scamware geschwächte Desktop-PCs, die den Fernzugriff per Remote Desktop Protocol (RDP)-Service erlauben.

Die Passwörter der Hacker

Doch recht erstaunlich ist, dass das mit Abstand am häufigsten ausgetestete Passwort ein einfaches "x" war, gefolgt von einem "Zz". Komplexere Phrasen wie "P@ssw0rd" und "&Tf45tUR@28" folgen abgeschlagen:

Die Passwörter der Hacker

1/10

Platz 1: x

Ein einfaches x scheint vielerorts schon zu genügen, um hineinzukommen.

Foto: Markus Gann - www.shutterstock.com

2/10

Platz 2: Zz

Wer sich ein wenig mit der Unix-Shell auskennt, weiß, dass der Texteditor vi zum Speichern von Dateien die Eingabe zweier großer Z verlangt. Ob dieses beliebte Passwort etwa daher rührt, ist nicht bekannt - die Ähnlichkeit ist jedoch verblüffend.

Foto: ariefpro - www.shutterstock.com

3/10

Platz 3: Start123

Ein typisches Standard-Passwort von Geräteherstellern. Wer es nicht ändert, ist selbst schuld.

Foto: Everett Historical - www.shutterstock.com

4/10

Platz 4: 1

Fast noch einfacher als das x, steht die 1 in der Liste nur auf 4.

Foto: arbuz - www.shutterstock.com

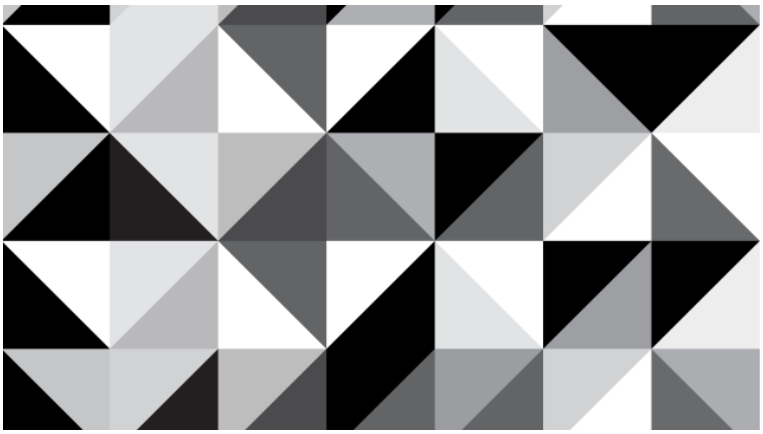
5/10

Platz 5: P@ssw0rd

Buchstaben durch Zahlen oder Sonderzeichen zu ersetzen, ist auch keine wirkliche Innovation...

Foto: Maxx-Studio - www.shutterstock.com

6/10



Platz 6: bl4ck4ndwhite

"It don't matter if you're black or white" sang Michael Jackson einst - hier spielt es auch keine Rolle, die kombinierte Farbenlehre sorgt aber durchaus für Hacker-Stimmung.

Foto: makicifu - www.shutterstock.com

7/10

Platz 7: admin

Der Klassiker darf natürlich nicht fehlen.

Foto: Yellowj - www.shutterstock.com

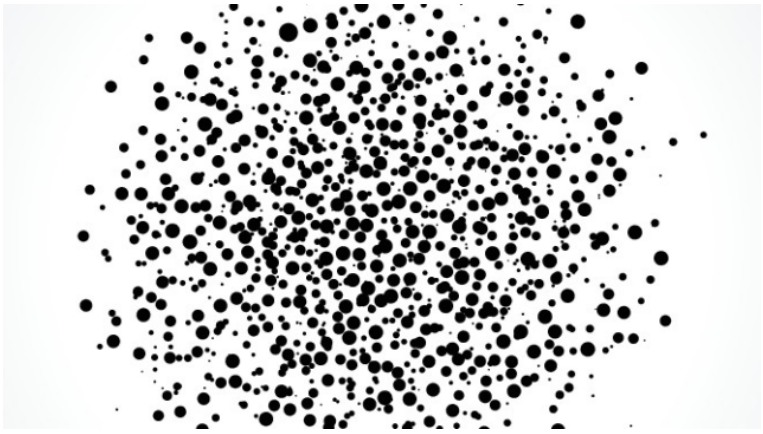
8/10

Platz 8: alex

Ob Tote-Hosen-Sänger Campino hier seine Hände mit im Spiel hat, ist äußerst unwahrscheinlich. Für viele Hacker-Routinen gilt trotzdem: Hier kommt Alex...

Foto: NarayTrace - www.shutterstock.com

9/10



Platz 9: .....

Über sieben Punkte musst du gehen...

Foto: Artishok - www.shutterstock.com

10/10

Platz 10: administrator

... und landest schließlich wieder beim IT-Experten schlechthin, dem Admin. Die Liste entstammt dem "Hacker's Dictionary" von Rapid7

Foto: LeoWolfert - www.shutterstock.com

Für die Nutzernamen gilt: "administrator" und "Administrator" liegen klar vor "user1" und "admin". Die am häufigsten verwendete Nutzername/Passwort-Kombination ist entsprechend "administrator / x". Die Häufigkeit, mit der Angreifer Nutzernamen wie ‘administrator/Administrator’, ‘pos’, ‘db2admin’ und ‘sql’ ausprobieren, impliziere laut Rapid7, dass Datenbanken und POS-Systeme unter den beliebtesten Angriffszielen sind.

Die Nutzernamen der Hacker

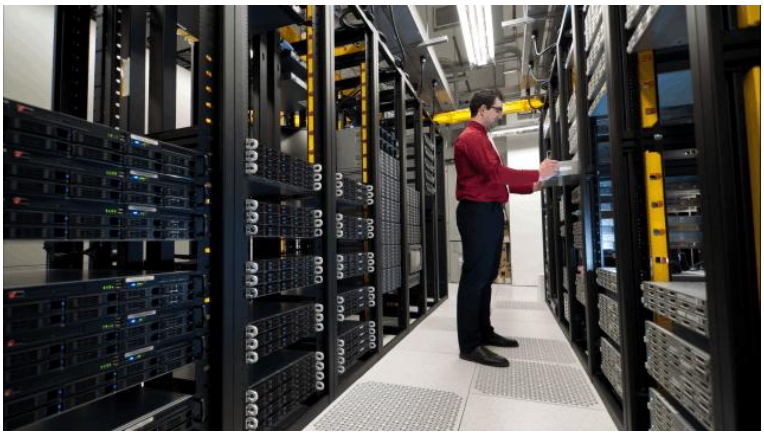
1/10

Platz 1: administrator

Der einfache "administrator" kommt in viele Systeme hinein...

Foto: Gajus - www.shutterstock.com

2/10



Platz 2: Administrator

... manchmal halt auch mit großem "A".

Foto: Arjuna Kodisinghe - www.shutterstock.com

3/10

Platz 3: user1

Und sollte der Administrator nichts helfen, bleibt immer noch der einfache Nutzer...

Foto: lassedesignen - www.shutterstock.com

4/10

Platz 4: admin

... und die Kurzform des Administrators.

Foto: Lagarto Film - www.shutterstock.com

5/10

Platz 5: alex

Alexander der Große hätte vielleicht seine Freude gehabt - genau wie bei den Hacker-Passwörten ist "alex" auch bei den Nutzernamen vorne mit dabei.

Foto: Vladimir Wrangel - www.shutterstock.com

6/10

Platz 6: pos

Weil sich viele der Angriffe auf Point-of-Sale-Systeme (PoS) beziehen, kann man es ja mal versuchen...

Foto: Sergiy Zavgorodny - www.shutterstock.com

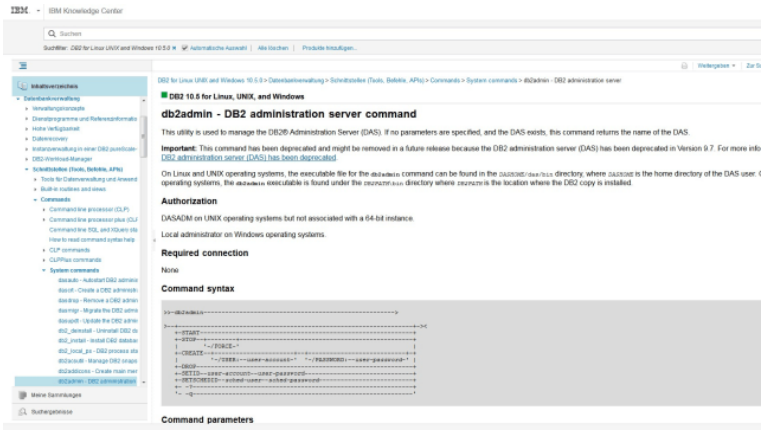
7/10

Platz 7: demo

Vielleicht existiert ja so etwas wie ein Musterzugang zu Demonstrationszwecken...

Foto: Rawpixel.com - www.shutterstock.com

8/10



Platz 8: db2admin

Der DB2 Administration Server der IBM lässt sich mit diesem Kommando verwalten. Kein Wunder also, dass dieser Nutzername in sämtlichen Hacker-Datenbanken auftaucht.

9/10

Platz 9: Admin

Wie gehabt.

Foto: docstockmedia - www.shutterstock.com

Platz 10: sql

SQL ist eine Datenbanksprache unter anderem zum Bearbeiten von Datenbeständen. Viele Webserver arbeiten damit - also durchaus verständlich, warum dies auch ein beliebter Nutzername ist. Die Liste entstammt dem "Hacker's Dictionary" von Rapid7

Foto: chrupka - www.shutterstock.com

Dass es mitunter ziemlich einfach sein muss, in anfällige Netze und Systeme einzudringen, liegt natürlich auch am Leichtsinn vieler Nutzer und Administratoren, die Standard-Passwörter der Hersteller nicht ändern, sich sehr einfach zu merkende Phrasen ausdenken und diese dann auch noch mehrfach verwenden.

Die am häufigsten gehackten Passwörter in den USA

Platz 25 bis 1

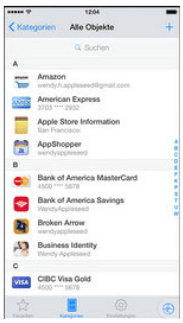
- 25. trustno1 ("Traueniemandem")
- 24. batman
- 23. 123123
- 22. 696969
- 21. superman
- 20. michael
- 19. master
- 18. shadow ("Schatten")
- 17. Access ("Zugang")
- 16. mustang
- 15. 111111
- 14. abc123
- 13. letmein ("Lassmichrein")
- 12. monkey ("Affe")
- 11. 1234567
- 10. Football
- 9. Dragon ("Drache")
- 8. baseball
- 7. 1234
- 6. 123456789
- 5. qwerty (auf deutschen Tastaturen "qwertz")
- 4. 12345678
- 3. 12345
- 2. password
- 123456

Passwort-Manager schaffen Abhilfe

Wer seine Passwörter sicherer machen möchte, ohne gleich einen Gedächtniswettbewerb gewinnen zu müssen, nutzt am besten einen Passwort-Manager. Welche zu empfehlen sind, haben wir abschließend für Sie zusammengestellt:

Empfehlenswerte Passwort-Manager für iOS

1/8



1Password

Dieser Passwort-Manager schützt Ihre Daten mittels authentifizierter AES 256-Bit-Verschlüsselung – das ist militärischer Standard. Dank automatischer Sperre sind Ihre Daten wie in einem Tresor weggesperrt, auch wenn Sie Ihr iPhone verlieren sollten oder es gestohlen wird. Mit dem Passwortgenerator lassen sich starke und einzigartige Passwörter erstellen, die alle an einer zentralen Stelle gesichert sind. Zusätzlich bietet die App eine direkte Integration in Safari und TouchID.

Preis: kostenlos: Zum Download

Foto: iTunes

2/8

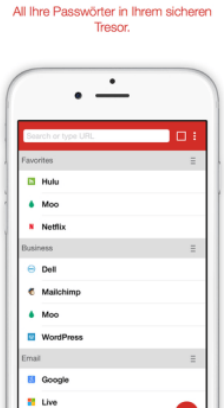
OneSafe

OneSafe gehört zu den besten Apps dieser Kategorie und kann neben Benutzername und Passwörtern auch Kreditkarten- und Kontodaten sowie Dokumente und Bilder sicher verwalten. Die App bietet neben iCloud auch die Möglichkeit der Synchronisierung über Dropbox. Auch oneSafe verwendet für die Speicherung der Daten den höchsten Sicherheitsstandard - die AES-256-Verschlüsselung.

Preis: 4,99 Euro: Zum Download

Foto: iTunes

3/8



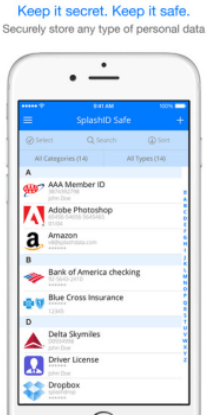
LastPass Password Manager

Auch die App LastPass gehört zu den besten Passwortmanager-Apps. Mit LastPass müssen Sie sich nur ein Passwort (Masterkennwort) merken, denn die App füllt Ihre Anmeldungen für Sie aus und synchronisiert Ihre Passwörter überall, wo Sie sie benötigen. Mit dem integrierten Passwort-Generator erstellen Sie ein garantiert sicheres Kennwort. Die App kann zwei Wochen lang kostenlos getestet werden, danach erfordert es den Premiumdienst. Dieser kostet 12 Dollar pro Jahr.

Preis: kostenlos: Zum Download

Foto: iTunes

4/8



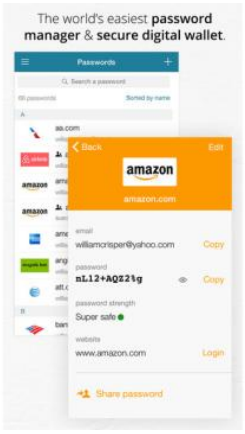
SplashID

In der kostenlosen App SplashID speichern Sie Ihre sensiblen Daten wie Web-Logins, Kreditkarten, PINs, E-Mail-Einstellungen, Lizenznummern und mehr mit der 256-Bit-AES-Verschlüsselung ab. Sodass Sie am Ende nur noch eine PIN für all Ihre Zugänge benötigen. Die gespeicherten Passwörter können Sie über iCloud, WLAN oder USB-Stick mit anderen Geräten synchronisieren. Leider gibt es keinen Excel-Export, um Daten weiterzuverarbeiten oder sie bei App-Wechsel mitumzuziehen.

Preis: kostenlos: Zum Download

Foto: iTunes

5/8



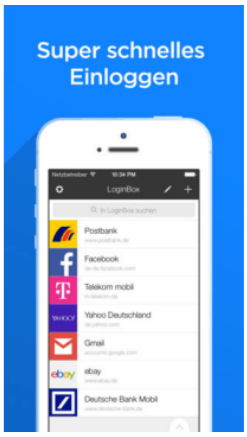
Dashlane

Nach dem Download von Dashlane muss ein Dashlane-Account angelegt werden. Hierbei sollten Sie schon auf ein sicheres Passwort achten, denn dieses verwenden Sie für Ihre Passwortliste. Auch hier wird die 256-AES-Verschlüsselung verwendet. Sollte Ihnen mal kein Kennwort einfallen, können Sie sich über die App ein unknackbares Kennwort generieren lassen. In der Premiumversion haben Sie noch die Möglichkeit Ihre Daten mit anderen Geräten zu synchronisieren. Hinweis: die App ist nur in den Sprachen Englisch, Französisch und Spanisch verfügbar.

Preis: kostenlos: Zum Download

Foto: iTunes

6/8



LoginBox Pro

Die App LoginBox kombiniert einen Passwort-Manager mit dem Browser und meldet Sie auf den gewünschten Internetseiten wie der Ihrer Bank, PayPal, eBay, Gmail, Punktesammel-Konten und weiteren mit nur einem Klick an. Das Besondere an dieser App ist der verminderte Klickaufwand, denn Sie müssen keine URLs, Benutzernamen oder Passwörter mehr eingeben. Dank der Sofortsuche werden die Webseiten noch schneller gefunden. Auch LoginBox ist mit dem höchsten Sicherheitsstandard ausgestattet.

Preis: 7,99 Euro: Zum Download

Foto: iTunes

7/8

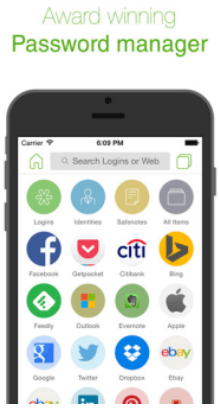
mSecure

Auch mSecure verwaltet Ihre Passwörter und synchronisiert sie über WLAN oder iCloud auf andere Geräte. Zur Verschlüsselung wird 256-Bit-Blowfish eingesetzt. Zu Beginn setzen Sie ein Masterpasswort für den App-Zugriff. Anschließend können Sie eine Liste mit Passwörtern und Login-Daten pflegen. Dank der Kategorisierung Ihrer Logins wie Privat und Geschäftlich haben Sie Ihre Daten immer im Überblick.

Preis: 9,99 Euro: Zum Download

Foto: iTunes

8/8



RoboForm

RoboForm übernimmt Benutzernamen und Passwörter, die Sie auf einer Webseite wie Ebay, Amazon oder Facebook eingeben und meldet Sie zukünftig automatisch dort an. Neben Zugangsdaten speichert die App auch persönliche Daten wie Ihre Adresse und Kontoinformationen ab, wodurch Sie Formulare per Drag and Drop ausfüllen können. RoboForm selbst sichern Sie mit einem Masterkennwort oder einer Touch-ID ab.

Preis: kostenlos: Zum Download

Foto: iTunes