Passwort-Knacker sind erfinderisch – Sie auch? Neue Erkenntnisse, die helfen.

Digitalisierung & IT

Von Michael Wolf

Jeder weiß es und macht es trotzdem nicht: sichere Passwörter erstellen, aufbewahren und verwalten. Alle, die regelmäßig im Internet unterwegs sind, betrifft es, und dennoch haben die wenigsten Nutzer wirklich die Nerven, sich mit dem Thema ernsthaft auseinander zu setzen – sollten sie aber. Insbesondere Unternehmen müssen Datensicherheit durch Passwörter ernst nehmen und alle Mitarbeiter, vom Geschäftsführer bis zum Pförtner, dafür sensibilisieren und schulen. Denn die Passwort-Knacker sind erfinderisch. Da es sich dabei nicht um Personen, sondern um clevere Programme handelt, die Profi-Hacker steuern, sind sie unserem Erfindungsreichtum bei Buchstaben und Ziffern meilenweit voraus und bekommen die meisten Passwörter mühelos geknackt. Doch welche Regeln sollte man anwenden? Was ist sicher und gleichzeitig praktikabel?

Michael Wolf

Kooperationspartner
Johannes Müller
Wirtschaftsberatung (BDU)

IT-Spezialist
IT-Architekt
Penetrationstests

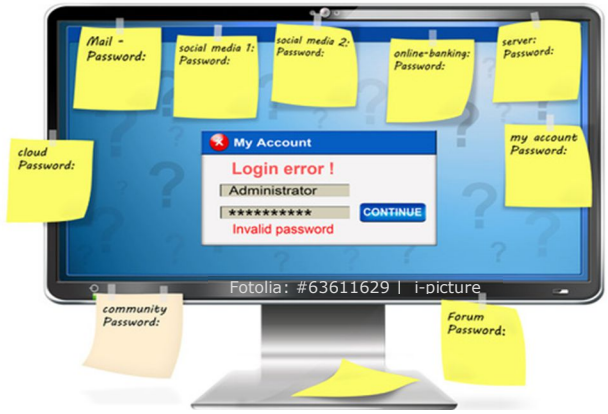
Das freut jeden Hacker: unsere Bequemlichkeit

Die Anzahl der Passwörter für die Anmeldung am PC, am Tablet, Notebook, smart Phone, bei Maschinen, der Firmensoftware oder bei privaten Transaktionen, wird immer größer. Je mehr Geräte wir im Einsatz haben und Geschäftsvorgänge online abwickeln, desto länger wird unsere Liste mit Kennwörtern, auf die wir täglich zugreifen müssen.

Da der Mensch von Haus aus faul ist, macht er es sich einfach und nimmt das gleiche Passwort für alle Zwecke. Die Fantasie und Zeit reichen gerade noch für ‚einfallsreiche' Variationen wie „passwort123" oder „passwort567", nicht jedoch für Zeichen- und Ziffernfolgen und schon gar nicht für regelmäßige Änderungen. Wer sich ein vermeintlich sicheres Passwort ausgedacht hat, kann es sich in der Regel nicht merken und notiert es womöglich – griffbereit – auf einem Post-it-Zettel am PC oder im Portemonnaie. Auch Excel-Tabellen sind ein beliebter Aufbewahrungsort, damit wechselnde Mitarbeiter schneller Zugriff auf alles bekommen.

„Kryptische Zeichenfolgen bei Passwörtern alleine helfen nicht. Auf die Länge kommt es an."

Doch Passwortsicherheit sollte immer an erster Stelle stehen, nicht die Bequemlichkeit. Einfache Merkregeln genügen bereits, um Passwörter zu erzeugen, die Ihre Datensicherheit enorm erhöhen. Nehmen Sie sich die Zeit, und überdenken Sie Ihre Passwörter.



Wie Sie es nicht machen sollten: Passwörter gehören weder an den PC, noch in Excellisten oder auf Zettel in der Geldbörse.

Sichere Passwörter erzeugen und aufbewahren

Die Regeln für Passwörter wurden inzwischen angepasst. Dafür hatte die US-Bundesbehörde NIST (National Institute of Standards and Technology) zuvor Millionen Vorfälle gehackter Passwörter ausgewertet. Bislang galt eine kryptische Zeichen- und Ziffernfolge als sicher. Nun sind sich die Experten einig, dass die alleinige Nutzung von Sonderzeichen, Groß- und Kleinschreibung und Zahlen keine große zusätzliche Sicherheit gebracht hat, sondern die Länge eines Passwortes ausschlaggebend ist. Auch der Hinweis, sein Passwort regelmäßig zu ändern, bringt nichts, wenn dabei das Kennwort nur minimal abgewandelt wird.

Nützliche Regeln bei der Passwortwahl

- je länger, desto besser (8 Zeichen reichen nicht!)
- keine Wörter aus dem Duden
- keine Vor- und Nachnamen, Tiernamen, Lieblingsstars, Geburtsdaten, usw.
- Groß- und Kleinschreibung, Ziffern und auch Sonderzeichen sind sinnvoll, jedoch clever verpackt, indem bspw. ein Satz mit Bezug auf den jeweilige Kontozugang als Passwort fungiert oder einzelne Buchstaben/Ziffern umgewandelt werden:

  Beispiel

  „Heiner h0rt gerne Jazz! Bei Goog1e.

  „Heiner h0rt gerne Jazz! Bei FB.

  Oder man nimmt den ersten Satz aus einem Buch auf einer bestimmten Seite, die man sich dann nur merken muss. Zusätzlich können Sie einzelne Buchstaben eines Satzes noch durch Zeichen oder Sonderzeichen ersetzen, wie im Bsp. oben „0" statt „ö", „1" statt „l" usw. Die Länge an sich ist jedoch wichtiger als die Verschlüsselung.

- keine Varianten, die sich aus der Tastatur ergeben, wie z.B. asfgh oder 12345äölkj
- keine voran- oder nachgestellte Sonderzeichen bei einfachen Passwörtern wie !Liebling! , §logmein? Oder %Lisa$

Schon gewusst?

Das meist genutzte Passwort der Welt lautet „password".

Dicht gefolgt von „123456" und „1234" …

Machen Sie das nicht!

Betrachten Sie Passwörter als wichtiges Element Ihrer Daten-sicherheits-maßnahmen.

Schulen Sie sich und alle Mitarbeiter!