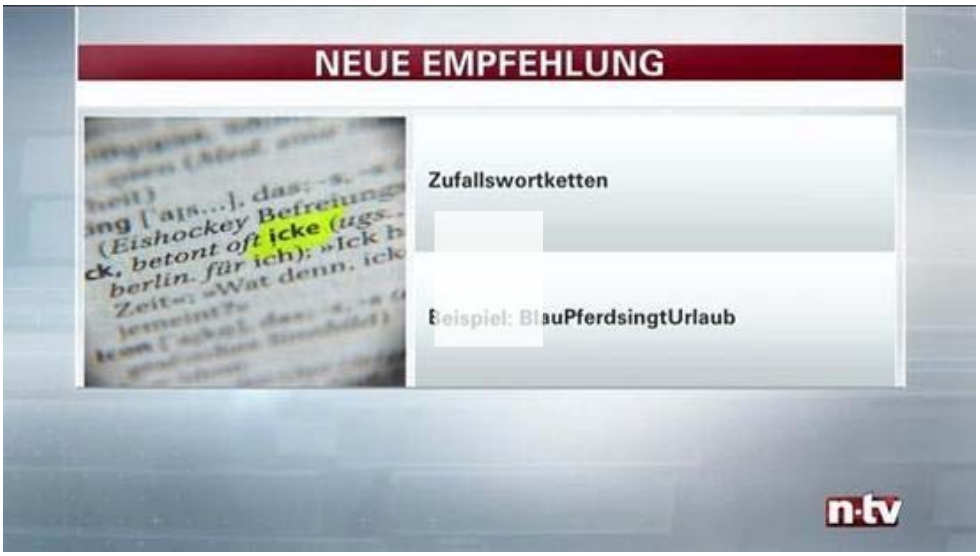
Handelsblatt

KOMPLIZIERTE REGELN FÜR PASSWÖRTER

Was für ein Un$1nn!

von: Christof Kerkmann
Datum: 12.08.2017 12:57 Uhr

Es liegt nicht an Ihnen: Die Regeln für Passwörter sind viel zu kompliziert. Nutzer dürfen aber darauf hoffen, dass es bald ohne Sonderzeichen und Ziffern geht. Die Standards stehen vor einer wichtigen Änderung.



IT-EXPERTE KLÄRT AUF
So sieht das perfekte Passwort aus

Düsseldorf. Das Internet ist voller Karikaturen über Passwörter. Da ist der Griesgram, der einer Wahrsagerin eine Liste mit allen Websites unter die Nase hält, für die er seine Zugangsdaten vergessen hat, während sie forschend in die Glaskugel blickt. Oder der strahlende Mann, der seine Kollegin wissen lässt, dass niemand sein Passwort erraten kann, weil es so kompliziert ist. Worauf sie antwortet: Ich lese es einfach vom Post-It am Monitor ab.

Die Witze zielen alle auf eine Tatsache ab: Passwörter sind die Pest. Wir müssen uns viel zu viele merken, und häufig sind wir gezwungen, bei der Festlegung komplizierten Regeln einhalten. Sonst mahnt uns das Buchhaltungssystem oder der E-Mail-Dienst: Zu kurz, keine Sonderzeichen, keine Ziffern, schon mal vorher genutzt. Was für ein Ärg3rni$!

Doch Nutzer dürfen auf eine gewisse Erleichterung hoffen: Im Juni hat die einflussreiche US-amerikanische Standardisierungsorganisation NIST ihre Empfehlungen angepasst. Es ist eine Entscheidung mit Signalwirkung: „Die NIST-Regeln haben auch im deutschsprachigen Raum eine sehr große Bedeutung“, sagt Arno Wacker, Professor für angewandte Informationssicherheit an der Universität Kassel. Nun werde an der gängigen Empfehlung gerüttelt.

SCHUTZ GEGEN DATENDIEBE

Passwörter gut schützen

Es klingt offensichtlich: Nutzer sollten ihre Passwörter gut schützen. Doch nicht wenige kleben ein Post-it mit Zugangsdaten an den Monitor oder speichern sie gar in einer Datei auf dem Rechner. Beides ist riskant – wenn Eindringlinge ins Büro oder auf den Rechner gelangen, können sie auch auf die E-Mails oder das Content Management System zugreifen.

Erst lesen, dann klicken

Es ist der Klassiker: In der E-Mail wird ein lustiges Katzenbild oder ein sensationelles Video angekündigt. Lädt man den Anhang herunter oder klickt auf den Link, fängt man sich aber einen Virus ein. Daher gilt nach wie vor die Regel, Anhänge und Links kritisch zu prüfen, ebenso Nachrichten von unbekannten Absendern.

Vorsicht mit USB-Sticks

Eine beliebte Angriffsmethode: Hacker lassen präparierte USB-Sticks auf dem Parkplatz oder in der Kantine liegen – und hoffen darauf, dass arglose Mitarbeiter das Gerät an den PC anschließen. Diese Masche funktioniert erschreckend gut. Die Lehre daraus: Nutzer sollten mit unbekannten Speichermedien extrem vorsichtig umgehen.

WLAN nur mit Verschlüsselung

Ob im Café oder am Flughafen: Wer mit seinem Smartphone oder Notebook ein öffentliches WLAN-Netzwerk nutzt, geht ein Risiko ein. Wenn man vertrauliche Daten abrufen will, sollte man das beispielsweise möglichst nur mit einer SSL-Verbindung tun. Weitere Tipps gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Schutz gegen Mitleser

In der Bahn oder im Flugzeug können Mitreisende ohne Probleme einen Blick auf das Notebook oder Smartphone erhaschen – und bekommen so möglicherweise sensible Informationen mit. Sicherheitsexperten raten daher, sich nach sogenannten Schultersurfern umzusehen und im Zweifelsfall die Datei geschlossen zu lassen. Zudem raten sie dringend davon ab, das Gerät auch nur kurz aus dem Auge zu lassen.

Gesunde Skepsis bei Apps

Apps können das Leben leichter machen, aber auch unsicherer: Viele Anwendungen fragen Informationen ab, die die Nutzer vermutlich nicht weitergeben wollen. Gerade Android-Nutzer sollten genau überprüfen, welche Berechtigungen ein Programm einfordert und im Zweifelsfall lieber die Finger davon lassen. Gleiches gilt für PC-Nutzer, die Programme aus dem Nutzer herunterladen und installieren. Besonders illegale Kopien sind häufig verseucht.

Code fürs Smartphone

Es mag zwar vielleicht nerven, wenn man jedes Mal einen Code eingeben muss, bevor man das Smartphone nutzen kann. Doch eine Sperre ist höchst nützlich, wenn das Gerät verloren geht oder gestohlen wird. Viele Firmen schreiben eine solche physische Absicherung vor. Im Büro kann es durchaus sinnvoll sein, den Rechner zu sperren, während man eine Besprechung hat oder in die Mittagspause geht.

Software aktuell halten

Auch dieser Tipp ist bekannt, er wird aber trotzdem oft nicht beherzigt: Nutzer sollten die Software auf ihrem Rechner immer aktuell halten. Das gilt nicht nur für den Virenscanner, sondern auch das Betriebssystem und Anwendungsprogramme wie Browser oder Textverarbeitung. Potentiell können Angreifer viele Lücken ausnutzen, um schädliche Software auf das Gerät zu schleusen.

Die Regeln, über die sich viele Karikaturisten lustig machen, stammen aus einem Dokument, das der NIST-Mitarbeiter Bill Burr 2003 aufsetzte. Unter Zeitdruck und ohne empirische Daten, wie er jetzt dem „Wall Street Journal“ beichtete (kostenpflichtiger Artikel). „Am Ende war es vermutlich für viele zu kompliziert“, sagte er. „Vieles von dem, was ich getan habe, bedaure ich jetzt“, erklärte der 72-

Jährige, der im Ruhestand ist.

Die gängigen Empfehlungen, basierend auf Burrs Regeln: Das Passwort sollte aus mindestens acht Zeichen bestehen und neben Buchstaben auch Ziffern und Sonderzeichen enthalten. Begriffe aus dem Wörterbuch sind dabei ebenso tabu wie Namen von Angehörigen oder Haustieren. Und am besten vergeben Nutzer alle paar Wochen oder Monate ein neues Passwort.

Das soll Hackern und Schnüfflern das Leben erschweren. Doch logisch ist nicht psychologisch. „Wenn Nutzer eine zufällige Sequenz aus mindestens acht oder besser noch zehn Zeichen bilden, ist das sehr sicher“, sagt zwar Passwort-Experte Arno Wacker im Gespräch mit dem Handelsblatt. Aber darunter leide die Benutzerfreundlichkeit: „Das kann sich kaum ein Mensch merken.“ Zumal, wenn diese Gedächtnisakrobatik alle 90 Tage aufs Neue ansteht.

MACHEN SIE DEN TEST
Elf Anzeichen, dass Sie gehackt wurden

Bild 1 von 24

Software installiert sich selbstständig
Ungewollte und unerwartete Installationsprozesse, die aus dem Nichts starten, sind ein starkes Anzeichen dafür, dass das System gehackt wurde. In den frühen Tagen der Malware waren die meisten Programme einfache Computerviren, die die "seriösen" Anwendungen veränderten - einfach um sich besser verstecken zu können. Heutzutage kommt Malware meist in Form von Trojanern und Würmern daher, die sich wie jede x-beliebige Software mittels einer Installationsroutine auf dem Rechner platziert. Häufig kommen sie "Huckepack" mit sauberen Programmen - also besser immer fleißig Lizenzvereinbarungen lesen, bevor eine Installation gestartet wird. In den meisten dieser Texte, die niemand liest, wird haarklein aufgeführt, welche Programme wie mitkommen.
(Foto: gms)

Daher haben die komplizierten Regeln mehrere unerwünschte Konsequenzen. So basteln sich viele Nutzer Begriffe zusammen, in denen Ausrufezeichen oder Ziffern einzelne Buchstaben ersetzen, und ändern diese jedes Mal nur leicht. Der Sicherheit dient das nicht: Hacker haben Programme, die solche Muster kennen und durchprobieren – wie ein automatischer Dietrich.

Nun ist es durchaus sinnvoll, den Nutzern Vorgaben zu machen. Das zeigt sich an den beliebtesten Passwörtern – Forscher können diese ermitteln, indem sie Daten analysieren, die Hacker ins Netz stellen. Zum Beispiel nach den massiven Cyberangriffen auf den Internetriesen Yahoo , den

Softwarehersteller Adobe oder den Seitensprungdienst Ashley Madison, bei denen in den vergangenen Jahren Millionen von Datensätzen an die Öffentlichkeit gelangten.

So verwenden viele Nutzer einfache Zahlenkombinationen und Begriffe, wie eine Auswertung des Hasso-Plattner-Instituts (HPI) in Potsdam zeigt. In den Top 10 deutschsprachiger Passwörter stehen „hallo“, „passwort“ und „schalke04“, außerdem „123456“ und „hallo123“. Weit oben stehen außerdem „arschloch“ und „ficken“. Hacker kennen diese Listen und schaffen es daher schnell, derartig nachlässige Absicherungen zu überwinden.

Doch wenn es zu kompliziert wird, dient das auch nicht der Sicherheit, wie der ehemalige NIST-Mitarbeiter Burr heute zugibt. Seine Nachfolger haben daher die Regeln angepasst. So erkennt die Organisation an, dass längere, aber einfach zu merkende Passphrasen mindestens genauso sicher sind wie kürzere, komplizierte Zeichenfolgen. Zumindest, wenn die enthaltenen Begriffe weitgehend zufällig ausgewählt sind. „correct horse battery staple“ (korrekt pferd batterie stapel) ist demnach sicherer als „Tr0ub4dor&3“, wie es die beliebte Comicreihe XKDC einmal ironisch auf den Punkt brachte.

xkcd: Password Strength https://t.co/oYtZOrSJ3b

Not actually that great, but better than most people's approach. pic.twitter.com/OZaHc2xXwh

— David C. Benson (@davidcbenson) 8. August 2017

IT-Sicherheitsexperte Wacker bestätigt das mit einer Überschlagsrechnung: Eine Phrase aus vier bis fünf einfachen Wörtern ermöglicht mehr Kombinationen als ein Wort aus acht Zeichen – und damit ist es für Kriminelle schwieriger, sie zu knacken, wenn sie denn weitgehend zufällig zusammengesetzt ist. „Für den Menschen ist es immer noch einfacher, sich so eine Abfolge zu merken, als ein komplexes Gebilde.“

Zudem hält die NIST nicht mehr daran fest, dass Passwörter nach einem bestimmten Zeitraum automatisch auslaufen. Die Online-Dienste und Softwareanbieter sollen eine Änderung nur noch dann erzwingen, wenn es ein Zeichen dafür gibt, dass sich jemand unerlaubt Zugriff auf die Daten verschaffen konnte.

Diese Position ist allerdings umstritten: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist darauf hin, dass es durchaus Argumente für ein Wechselintervall gebe. So bemerken Nutzer wie Firmen häufig nicht oder erst spät, dass sich Cyberkriminelle Zugriff auf die Daten verschafft haben. In der Zeit haben sie freie Bahn. Die IT-Spezialisten aus Bonn raten zur Differenzierung, abhängig vom „Schutzbedarf der jeweiligen IT-Systeme“.

Die neuen Erkenntnisse könnten bald auch deutschen Nutzern vermehrt zugutekommen. „Die IT-Verantwortlichen werden diese Meldung alle gelesen haben und intern Überlegungen anstellen, wie sie ihre eigenen Passwortrichtlinien verbessern können“, sagt Peter Meyer, der beim Verband der Internetwirtschaft Eco den Bereich IT-Sicherheitsservices leitet. Die Umsetzung sei allerdings nicht immer trivial, weil die Systeme angepasst werden müssten - bei einem Konzern mit Tausenden Mitarbeitern ist das nicht immer so einfach. Grundsätzlich sieht der Experte viele Unternehmen aber bereits auf einem guten Weg: Sie setzen etliche der neuen Empfehlungen bereits um.

WIE DIE HACKER ZUM ZIEL KOMMEN

Eine einzige Schwachstelle reicht

Wenn kriminelle Angreifer in ein Computersystem eindringen wollen, haben sie einen Vorteil: Sie müssen womöglich nur eine einzige Schwachstelle finden, um einen Rechner zu kompromittieren. Einige ausgewählte Angriffsmethoden.

Verspätetes Update

Es gibt praktisch keine fehlerlose Software – wenn Sicherheitslücken entdeckt werden, sollte sie der Hersteller mit einem Update schließen. Viele Firmen lassen sich jedoch Zeit, diese zu installieren und öffnen Angreifern somit Tür und Tor.

Angriff auf die Neugier

Der Mensch ist neugierig - das machen sich kriminelle Hacker zunutze: Sie verfassen fingierte E-Mails, die wichtige Dokumente oder ein lustiges Video versprechen, aber nebenbei die Zugangsdaten eines Mitarbeiters stehlen. Phishing wird diese Methode genannt.

Gutgläubigkeit als Einfallstor

„Hier ist die IT-Abteilung. Wir brauchen mal Ihr Passwort“: Nicht selten gelangen Angreifer mit einem dreisten Anruf an die Zugangsdaten eines Mitarbeiters. Wer gutgläubig ist, fällt auf diese Masche rein – obwohl die IT-Fachleute aus dem eigenen Haus nie so eine Frage stellen würden.

Ein Passwort, das nicht sicher ist

Ob Router oder Drucker: Viele Geräte werden mit einem Standardpasswort ausgeliefert. Wenn die IT-Abteilung es nicht verändert, haben Angreifer leichtes Spiel. „Die Handbücher mit dem Passwort stehen oft im Internet“, sagt Joachim Müller, Chef für IT-Sicherheit beim Dienstleister Ceyoniq Consulting.

Ein schwaches Glied

Angreifer suchen das schwächste Glied in der Kette, häufig alte Systeme. Zudem kennen professionelle Angreifer – neben Kriminellen auch Geheimdienste – oft Sicherheitslücken, die den Herstellern der Software noch nicht bekannt sind. Gegen solche Zero-Day-Exploits kann man sich kaum schützen.

Alle Probleme können die neuen Regeln indes nicht beheben. Denn weiterhin gilt die Empfehlung, für die verschiedenen Programme und Online-Dienste einzigartige Passwörter zu verwenden. Kein Wunder, dass sich mehr als ein Drittel der Internetnutzer davon überfordert fühlt, wie der Bitkom im vergangenen Jahr erhoben hat. IT-Sicherheitsexperte Wacker empfiehlt daher Passwortmanager, um einen Großteil der Zugangsdaten automatisch zu verwalten und das Gedächtnis zu entlasten. „Nur für die Dienste, die ich viel nutze, merke ich mir die Passphrasen“, erläutert der Experte. Der größte Gram lässt sich damit vermeiden.