Bundesamt für Sicherheit in der Informationstechnik

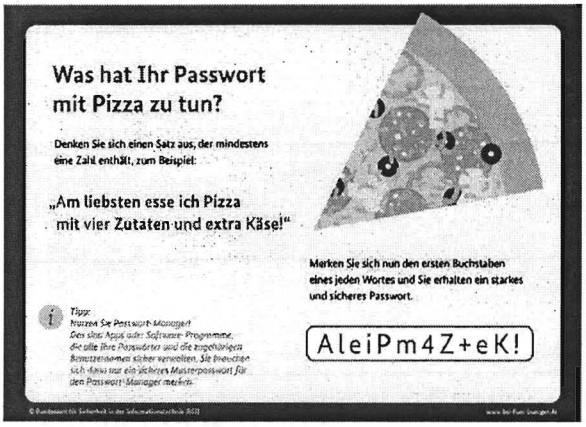
BSI FÜR BÜRGER
INS INTERNET - MIT SICHERHEIT

Passwörter

Wer die Wahl hat, hat die Qual – heißt es. Besonders bei der **Wahl der richtigen Passwörter** tun sich viele Internetnutzer schwer. Wen wundert's da, dass schlecht gewählte Passwörter wie 123456 oder qwert auf der Hitliste besonders häufiger IT-Sicherheitsdefizite ganz weit oben stehen? Bei denen, die sich stattdessen die Mühe machen, ein etwas komplizierteres Passwort zu nutzen, kommt es nicht selten vor, dass ein und dasselbe Passwort für viele verschiedene Programme beziehungsweise Zugänge genutzt wird. Hacker freut das alles natürlich. Sie haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren, ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen oder einmal im Internet veröffentlichte Zugangsdaten bei allen möglichen Diensten durchprobieren. Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen und immer nur für einen Zugang genutzt werden.

Hinzu kommt, dass Passwörter nicht nur zum Schutz von vertraulichen Daten dienen. Ein Beispiel: Inzwischen ist es üblich, dass man sich bei unterschiedlichsten Anbietern im Internet ein Konto oder einen Zugang (Account) anlegen kann. Die Anmeldung an diesem Account wird mit einem Passwort geschützt. Was könnte passieren, wenn sich jemand unter Ihrem Namen dort anmeldet? Wer möchte schon gerne, dass Fremde unter dem eigenen Namen E-Mails verschicken oder teure Waren im Internet ersteigern können?

Deshalb: Orientieren Sie sich an den folgenden Empfehlungen zur Erstellung und zum Umgang mit Passwörtern – und schon tun Sie etwas für Ihre Sicherheit.



Quelle: *Bundesamt für Sicherheit in der Informationstechnik (BSI)*

Tipps für ein gutes Passwort

- Bei der Wahl eines Passwortes sind Ihrer Kreativität keine Grenzen gesetzt. Wichtig ist, dass Sie sich **das Passwort gut merken können**. Hierfür gibt es unterschiedliche Hilfsstrategien: Der eine merkt sich einen Satz und benutzt von jedem Wort nur den 1. Buchstaben (oder nur den zweiten oder letzten). Anschließend verwandelt man unter Umständen noch bestimmte Buchstaben in Zahlen oder Sonderzeichen. Die andere nutzt einen ganzen Satz als Passwort oder reiht unterschiedliche Wörter, verbunden durch Sonderzeichen, aneinander. Eine weitere Möglichkeit besteht darin, zufällig 5-6 Worte aus dem Wörterbuch zu wählen und diese mit einem Leerzeichen zu trennen. Dies resultiert in einem leicht zu merkenden, leicht zu tippenden und für Angreifer schwer zu brechenden Passwort.
- Grundsätzlich gilt: **Je länger, desto besser**. Ein gutes Passwort sollte **mindestens acht Zeichen** lang sein. Bei Verschlüsselungsverfahren für WLAN wie zum Beispiel WPA und WPA2 sollte das Passwort beispielsweise mindestens 20 Zeichen lang sein. Hier sind so genannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren.
- Für ein Passwort können in der Regel **alle verfügbaren Zeichen** genutzt werden, beispielsweise **Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...)**. Manche Anbieter von Onlinediensten machen technische Vorgaben für die verwendbaren bzw. zu verwendenden Zeichen. Wenn Ihr System Umlaute zulässt, bedenken Sie bei Reisen ins Ausland, dass auf landestypischen Tastaturen diese eventuell nicht eingegeben werden können.
- Nicht als Passwörter geeignet sind Namen von Familienmitgliedern, des Haustiers, des besten Freundes, des Lieblingsstars, Geburtsdaten und so weiter. Das vollständige Passwort sollte möglichst **nicht in Wörterbüchern** vorkommen. Es sollte zudem nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern wie "asdfgh" oder "1234abcd" bestehen. Manche Anbieter gleichen Passwörter gegen eine sogenannte "black list" ab, in der genau solche nicht geeigneten Passwörter hinterlegt sind. Möchte man sie nutzen, erhält man einen Hinweis, dass das Passwort in dieser Form nicht zugelassen wird bzw. nicht sicher ist.
- Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? # am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen, ist nicht empfehlenswert.
- Wichtige Passwörter sollten in regelmäßigen Abständen geändert werden. Warum, erklären wir unter Umgang mit Passwörtern.
- Nutzen Sie einen Passwortmanager, um Ihre unterschiedlichen Passwörter gut verwalten zu können. – und ihr starkes Passwort, um diesen abzusichern. So müssen Sie sich nur ein gutes Passwort merken und können trotzdem sehr starke, überall unterschiedliche Passwörter verwenden.