KATHOLISCH
Bistum Mainz

02

[Merkblatt zur Passwortgestaltung und –verwendung]

einfach & sicher

Datenschutz im Bistum Mainz

Betriebliche Datenschutzstelle
Stand: November 2023

[Merkblatt zur Passwortgestaltung und –verwendung]

Hinweise zur sicheren Passwortgestaltung [1]

PC, Laptop, Smartphone: Wir befinden uns mitten im digitalen Zeitalter und die meisten Menschen sind immer und überall vernetzt. Gerade das World Wide Web aber birgt zahlreiche Gefahren für die Privatsphäre eines jeden. Zahlreiche Schadsoftware zieht täglich ihre Bahnen durch das Internet und erreicht nicht nur über das elektronische Postfach die teils arglosen User.

Um sensible Daten wie Bankverbindungen, aber auch andere personenbezogene Daten und private Bilderschätze gegen potentielle Angriffe besser zu schützen, kommt der Passwort-Sicherheit ein immer höherer Stellenwert zu. Doch auch bei der Wahl eines Passwortes sind viele noch immer zu nachlässig. Auch weiterhin lassen die beliebtesten Eingaben die nötige Passwortstärke vermissen.
Nach einer Erhebung des Hasso-Platter-Instituts für Softwaresystemtechnik (HPI) zeigte sich, dass auch 2016 noch die beliebtesten Passwörter alles andere als sicher sind. Hier die Top 8 in Deutschland:

hallo
passwort
hallo123
schalke04
passwort1
qwertz
schatz
hallo1

Kreativität Fehlanzeige! Um Hackern nicht Tür und Tor zu öffnen, sollten Sie grundsätzlich von allzu leichten Passwörtern Abstand nehmen.

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 dem 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.

Die Infografik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zeigt, wie man sich ein möglichst komplexes Passwort gut merken kann.

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.

Umgang mit Passwörtern

Passwörter notieren?

Passwörter sollten niemals unverschlüsselt auf dem PC abgelegt werden oder auf dem berühmten Notizzettel am Bildschirm kleben. Wer sich Passwörter notieren will, sollte sie stattdessen gut unter Verschluss halten bzw. auf dem Rechner in einer verschlüsselten Datei ablegen.
Wer viele Online-Accounts hat, für den empfiehlt sich ein Passwort-Verwaltungsprogramm wie zum Beispiel keepass (eine deutsche Sprachdatei für dieses englischsprachige Programm gibt es auf der Herstellerseite). Diese Programme können neben der Passwort-Verwaltung auch starke Passwörter generieren (berücksichtigen Sie bei den Einstellmöglichkeiten zur Passwortgenerierung unsere oben genannten Mindestempfehlungen). Sie müssen sich dann nur noch ein gutes Masterpasswort überlegen und merken.

Wie merkt man sich ein gutes Passwort?

Auch dafür gibt es Tricks. Eine beliebte Methode funktioniert so: Man denkt sich einen Satz aus und benutzt von jedem Wort nur den 1. Buchstaben (oder nur den zweiten oder letzten). Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen. Hier ein Beispiel:

"Morgens stehe ich auf und putze mir meine Zähne drei Minuten lang." Nur die ersten Buchstaben: "MsiaupmmZdMl". "i und l" sieht aus wie "1", "&" ersetzt das "und": "Ms1a&pmmZ3M1".

Oder, hier dir Bistums Variante: „Sankt Martin, dir ist anvertraut das Volk des Herrn“ aus dem neuen Gotteslob auf Seite 926

„StMd1adVdHnGl926“

Auf diese Weise hat man sich eine gute "Eselsbrücke" gebaut. Natürlich gibt es viele andere Tricks und Methoden, die genauso gut funktionieren, etwa das Aneinanderreihen von beliebigen, zusammenhanglosen Wörtern. Ein Beispiel - was Sie dann natürlich nicht selbst verwenden sollten: "Ein blaues Pferd liest Kaffeesatz auf dem Ausflugsdampfer".

Außerdem ist es ratsam, dass sich der Benutzer des Passwortes den Satz selbst ausgedacht hat. Wird als Merksatz zum Beispiel ein bekanntes Literaturzitat oder eine Liedzeile als Passwort gewählt, so ist es wahrscheinlich, dass Angreifer auch dies mittels einer Wörterbuchattacke herausfinden können.

Änderung von Passwörtern

Zunächst sollten Sie sich Gedanken machen, welche Ihrer Passwörter besonders viele oder sensible persönliche Daten schützen. Ein wichtiges Passwort ist zum Beispiel Ihr Passwort für Ihr privates E-Mail-Konto. Dort sind nicht nur persönliche Nachrichten und Kontakte hinterlegt, sondern mithilfe des Zugangs zu Ihrem E-Mail-Account lassen sich auch viele andere Passwörter in von Ihnen genutzten Online-Diensten zurücksetzen und neu vergeben. Andere Beispiele für wichtige Passwörter sind das Passwörter für ihre dienstlichen Zugänge oder die Passwörter für Profile in sozialen Netzwerken, für den Zugang zu häufig genutzten Online-Shops oder andere regelmäßig genutzte elektronische Identitäten. Diese wichtigen Passwörter sollten in regelmäßigen Zeitabständen geändert werden, mindestens einmal jährlich. Eine solche eigenständige Änderung ohne externen Anlass macht Ihre Zugangsdaten für Dritte wertlos, sollten sie ohne Ihr Wissen entwendet worden sein. Einige Programme und Dienstleister erinnern Sie automatisch daran, wenn Sie das Passwort schon längere Zeit benutzen.

Ein Passwort sollte auf jeden Fall geändert werden, wenn es einen Hinweis gibt, dass es tatsächlich in die Hände von unbefugten Dritten gelangt ist. Ein solcher Hinweis kann beispielsweise die direkte Aufforderung eines Dienstanbieters sein, das Passwort zu ändern, ebenso die Nachricht, dass Passwörter eines bestimmten Dienstleisters gestohlen worden

und nun im Internet aufgetaucht sind. Auch eine Spam- oder Phishing-Mail, in der korrekte persönliche Daten genutzt werden, kann ein Hinweis darauf sein, dass jemand Zugang zu einem privaten Account hatte und dort Daten abgriff.

Sollten Sie feststellen, dass Ihr Gerät mit einem Schadprogramm infiziert ist, ist dies ebenfalls ein Grund, Passwörter zu ändern. Manche Varianten von Schadprogrammen zeichnen Zugangsdaten auf und übermitteln diese an Dritte. Um dies zu unterbinden, muss zunächst das Gerät bereinigt werden. Erst anschließend sollten die Passwörter geändert und Log-Ins wieder über das betroffene Gerät durchgeführt werden.

Zugangsdaten, die Cyber-Kriminelle bei Anbietern oder direkt bei Nutzerinnen und Nutzern abgegriffen haben, werden anschließend oft im Internet veröffentlicht oder zum Kauf angeboten. Diese Datensätze kursieren dann im Netz. Je länger darin enthaltene Zugangsdaten nicht geändert werden, desto mehr Dritte können sie für ihre Zwecke nutzen. Im Internet gibt es unterschiedliche Portale, über die überprüft werden kann, ob persönliche Zugangsdaten in einem solchen bekanntgewordenen Datensatz enthalten sind. Ein deutschsprachiges Angebot ist beispielsweise der HPI Identity Leak Checker, ein internationaler Anbieter haveibeenpwned.com. Das BSI kann keine Aussage zu der Qualität und Aktualität der dort hinterlegten Daten treffen. Grundsätzlich ist bei der Nutzung solcher Portale zu beachten, dass für Zugangsdaten häufig die Kombination aus E-Mail-Adresse und Passwort verwendet wird. In den Datenbanken wird allerdings in der Regel nur die E-Mail-Adresse mit dem Datenbestand abgeglichen. Die Rückmeldung, dass die E-Mail-Adresse in dem Datenbestand enthalten ist, kann sich also auf jeden Account beziehen, bei dem diese E-Mail-Adresse zum Zugang genutzt wird, eine direkte Zuordnung ist nicht möglich.

Keine einheitlichen Passwörter verwenden

Viele Anwender denken sich ein Passwort aus und nutzen dieses dann für mehrere Online-Accounts, damit sie sich nicht viele verschiedene Passwörter merken müssen. Dieser Ansatz ist bequem, aber dennoch nicht zu empfehlen, selbst wenn das gewählte Passwort den oben genannten Kriterien entspricht. Denn gerät das Passwort einer einzelnen Anwendung in falsche Hände, hat der Angreifer freie Bahn für alle weiteren Accounts mit dem gleichen Passwort. Er kann einfach automatisiert durchtesten, wo dieses Passwort ebenfalls verwendet wird.

Voreingestellte Passwörter ändern

Bei vielen Softwareprodukten werden bei der Installation (beziehungsweise im Auslieferungszustand) in den Accounts leere Passwörter oder allgemein bekannte Passwörter verwendet. Hacker wissen das: Bei einem Angriff probieren sie zunächst aus, ob vergessen wurde, diese Accounts mit neuen Passwörtern zu versehen. Deshalb ist es ratsam, in den Handbüchern nachzulesen, ob solche Accounts vorhanden sind und wenn ja, die voreingestellten Passwörter zu ändern.

Bildschirmschoner mit Kennwort sichern

Bei den gängigen Betriebssystemen haben Sie die Möglichkeit, Tastatur und Bildschirm nach einer gewissen Wartezeit zu sperren. Die Entsperrung erfolgt erst nach Eingabe eines korrekten Passwortes. Diese Möglichkeit sollten Sie nutzen. Ohne Passwortsicherung können unbefugte Dritte sonst bei vorübergehender Abwesenheit des rechtmäßigen Benutzers Zugang zu dessen PC erlangen. Natürlich ist es störend, wenn die Sperre schon nach kurzer Zeit erfolgt. Unsere Empfehlung: Fünf Minuten nach der letzten Benutzereingabe sollte der Bildschirmschoner anspringen und damit die Sperrung erfolgen. Zusätzlich gibt es die Möglichkeit, die Sperre im Bedarfsfall auch sofort zu aktivieren. Bei einigen Windows-Betriebssystemen erfolgt dies beispielsweise durch die Tastenkombination Strg+Alt+Entf.

Passwörter nicht an Dritte weitergeben oder per E-Mail versenden!

In der Regel werden E-Mails unverschlüsselt versandt und können so von Dritten auf ihrem Weg durch das Internet mitgelesen werden. Zudem können E-Mails im Internet verloren gehen oder herausgefiltert werden. Der Absender einer E-Mail hat daher keine Gewissheit, dass seine Nachricht den gewünschten Empfänger auch wirklich erreicht hat. Aus diesen Gründen sollten Sie Passwörter nicht per E-Mail versenden.

Grundsätzlich gilt: Geben Sie Ihre Passwörter an Dritte weiter, verlieren Sie die Kontrolle, weil diese Dritten nun theoretisch die entsprechenden Dienste nutzen und die dort hinterlegten Informationen ändern könnten. So haben Sie sich umsonst die Mühe für ein gutes Passwort gemacht.

Quellen: www.datenschutz-mv.de, www.datenschutz.org, www.bsi-fuer-buerger.de, www.sueddeutsche.de,

[1] Nach: Bundesamt für Sicherheit in der Informationstechnik

Impressum:

Herausgegeben vom
Bischöflichen Ordinariat Mainz

KATHOLISCH
Bistum Mainz

Betriebliche Datenschutzstelle im Bistum Mainz
☎ 06131-253857
✉ Postfach 1560, 55005 Mainz
datenschutz@bistum-mainz.de

Redaktion: Wolfgang Knauer, Alexandra Glinka

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Basisschutz: Sichere Passwörter

Passwörter begleiten uns täglich und trotzdem oder gerade deshalb greifen viele Menschen bei der Wahl ihrer Passwörter auf einfache Zahlenabfolgen oder Namen und Orte in Kombination mit Zahlen oder Sonderzeichen zurück. Diese sind zwar leicht zu merken, können aber ebenso leicht von Cyber-Kriminellen geknackt werden.

Bei einem Cyber-Angriff sind nicht nur persönliche Daten und sensible Informationen in Gefahr, Cyber-Kriminelle können die gehackten Accounts auch für kriminelle Machenschaften und illegale Geschäfte nutzen. Um das zu verhindern, sollte ein Passwort bestimmte Anforderungen erfüllen und immer nur für einen Zugang genutzt werden.

Grundsätzlich können Sie zwei Strategien anwenden, um ein sicheres Passwort zu erstellen:

Weitere Informationen:
https://www.bsi.bund.de/dok/6596574

Sicheres Passwort

Kurzes, dafür komplexes Passwort

- Ist acht bis zwölf Zeichen lang.
- Besteht aus vier verschiedenen Zeichenarten.
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen werden willkürlich aneinandergereiht.

Langes, dafür weniger komplexes Passwort

- Ist mindestens 25 Zeichen lang.
- Besteht aus zwei Zeichenarten.
- Kann zum Beispiel aus sechs aufeinanderfolgenden Wörtern bestehen, die jeweils durch ein Zeichen voneinander getrennt sind.

Um ihre Accounts und Daten zu schützen, sollten Sie außerdem folgende Tipps beherzigen:

Generell gilt

- ✓ Ein individuelles Passwort pro Account!
- ✓ Eine Mehr-Faktor-Authentisierung (ergänzend zum Passwort durch bspw. eine Gesichtserkennung, eine App-Bestätigung, E-Mail oder einer PIN auf einem anderen Gerät) ist empfehlenswert.
- ✓ Alle verfügbaren Zeichen nutzen inklusive Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...).
- ✓ Das vollständige Passwort sollte nicht im Wörterbuch vorkommen.

Zu vermeiden

- ✗ Namen von Familienmitgliedern, Haustieren, Geburtsdaten etc.
- ✗ Einfache oder bekannte Wiederholungs- bzw. Tastaturmuster wie „asdfgh“ oder „1234abcd“
- ✗ Ziffern oder Sonderzeichen an den Anfang oder ans Ende eines ansonsten einfachen Passwortes.
- ✗ Dasselbe Passwort bei mehr als einem Account.

Merkblatt zur Passwortgestaltung und –verwendung,