Umgang mit Zugangsdaten und Passwörtern

IV-Sicherheitsteam, Oktober 2017
https://www.uni-muenster.de/IV-Sicherheit

Einleitung

Passwörter sind ein leidiges Thema. Schon beim Einschalten des Computers wird man danach gefragt und danach wird es nicht besser. Sie wollen Ihre E-Mails lesen? Bitte geben Sie Ihr Passwort ein. Sie wollen etwas bestellen? Bitte geben Sie Ihr Passwort ein. Von allen Seiten wird man mit ihnen konfrontiert und überall werden Bedingungen und Anforderungen an diese gestellt. Aber wieso das alles?

Passwörter oder genauer Zugangsdaten, also die Kombination aus Benutzernamen und Passwörtern, sind heutzutage die am weitesten verbreitete Methode, um sich bei zugriffgeschützten Geräten oder persönlichen Diensten anzumelden. Unter diese Geräte und Dienste fallen viele Dinge, mit denen Sie wahrscheinlich täglich zu tun haben, wie z.B. Ihr Computer, der Zugriff auf Netzlaufwerke, das Abrufen Ihrer E-Mails, aber auch die MeinZIV-Seite, Online-Shops oder ein Online-Banking-Portal Ihrer Bank. Das heißt, dass nur die Kenntnis über korrekte Zugangsdaten den Zugriff ermöglicht und Sie dem Dienst gegenüber identifiziert.

Inhaltsverzeichnis

Was kann Ihnen passieren?

Wahrscheinlich war Ihnen dieser Umstand bereits bewusst, warum sollten Sie also noch weiterlesen? Nur Sie kennen doch Ihre Zugangsdaten, was soll da also schon passieren? Natürlich kennen im idealen Fall nur Sie selbst Ihre Zugangsdaten, aber was passiert, wenn jemand anderes diese Daten doch erlangen sollte? Dies passiert heutzutage sogar recht häufig und die meisten Menschen sind sich nicht über die Ausmaße der Konsequenzen bewusst, denn Passwörter schützen nicht nur vertrauliche Daten. Vor Allem, wenn die selben Passwörter bei verschiedenen Diensten genutzt werden, können Dritte viel Unheil anrichten, das nicht nur Ihnen persönlich, sondern auch der WWU oder anderen Unternehmen schaden kann. Was könnte ein Angreifer denn zum Beispiel mit Ihren MeinZIV-Zugangsdaten anfangen? Dieser könnte zum Beispiel...

- Änderungen in der Budgetverwaltung vornehmen
- den Print&Pay-Dienst auf Ihre Kosten nutzen
- Prüfungen für Sie an- oder abmelden
- persönliche Informationen über Sie auslesen
- Zugriff auf Ihre Daten auf dem U-Laufwerk
- Ihre E-Mails mitlesen
- E-Mails in Ihrem Namen verschicken

Aber ein Angreifer würde hier nicht Halt machen, sondern wird versuchen, die erlangten Zugangsdaten auch bei anderen populären Diensten, wie Internet-Foren, anderen E-Mail-Anbietern, Messaging-Diensten oder Online-Shops, einzusetzen. Sollten Sie das selbe Passwort auch bei anderen Diensten nutzen, könnte der Angreifer auch...

- teure Waren oder Dienstleistungen auf Ihre Kosten bestellen
- Ihre Daten in sciebo löschen
- in Ihrem Namen über Messaging-Dienste/Soziale Netzwerke kommunizieren
- Ihre Freunde und Bekannte "angreifen" (Rufschädigung)
- auf Ihre Daten in Cloud-Speichern zugreifen
- Sie aus Diensten aussperren ("Geiselnahme") durch Ändern des Passworts

Wie kommen Kriminelle an Ihr Passwort?

Phishing

Doch wie sollte ein Angreifer überhaupt Ihr Passwort erlangen? Häufig versuchen Kriminelle über sogenannte Phishing-E-Mails oder -Internetseiten Sie dazu zu bringen, Ihre Zugangsdaten auf präparierten Internetseiten einzugeben, die diese direkt an die Angreifer verschickt.

Schadsoftware

Auch durch Schadsoftware auf Ihrem Computer oder Smartphone können eingegebene Passwörter ausgelesen werden. Außerdem können Zugangsdaten durch Angriffe auf schlecht abgesicherte Datenbanken, die Zugangsdaten von Diensten enthalten, oder schlecht abgesicherte Verbindungen entwendet werden. Dagegen hilft nur ein sicherer Umgang mit Passwörtern (s.u.).

Brute Force

Eine letzte Möglichkeit ist das Ausprobieren von Passwörtern mit roher Gewalt (engl. „brute force“). Häufig sind Benutzernamen einfach E-Mail-Adressen oder lassen sich erahnen, sodass nur noch das Passwort fehlt. Angreifer können nun versuchen, dieses durch automatisiertes Ausprobieren, sogenannte Brute-Force-Angriffe, von bekannten Passwörtern oder häufig genutzten Kombinationen zu erhalten. Mit wenig Aufwand lassen sich riesige Listen bekannter Passwörter erlangen, beispielsweise auch die 10 häufigsten deutschen Passwörter:

"Top Ten" deutscher Passwörter

1. hallo	6. qwertz
2. passwort	7. arschloch
3. hallo123	8. schatz
4. schalke04	9. hallo1
5. passwort1	10. ficken

Abbildung 1 - "Top Ten" deutscher Passwörter (Quelle: hpi.de)

Um gegen das Ausprobieren bekannter Passwörter geschützt zu sein, müssen sichere Passwörter genutzt werden.

Wie können Sie sich schützen?

Passwortdiebstahl kann sehr lukrativ für Kriminelle sein. Um es Kriminellen zu erschweren und Ihre Zugänge möglichst gut abzusichern, haben wir einige grundlegende Empfehlungen zusammengestellt.

Umgang mit Passwörtern/Sichere Webseiten

Zuallererst sollten Sie einige wichtige Regeln zum Umgang mit Passwörtern beachten, die Sie vor allem vor Phishing-Angriffen schützen:

- Verwenden Sie für unterschiedliche Dienste (Uni, Amazon, Google, eBay etc.) unterschiedliche Passwörter
- Geben Sie Ihr Uni-Passwort nur auf Uni-Webseiten ein!
- Geben Sie Ihre Passwörter nur auf verschlüsselten (grünes Schloss in der Adressleiste bzw. https statt des normalen http am Anfang der www-Adresse) und vertrauenswürdigen (plausible www-Adresse) Webseiten ein!
- Geben Sie Passwörter nur auf vertrauenswürdigen Geräten ein, die mit den grundsätzlichen Sicherheitsmaßnahmen (Antivirus-Software und Firewall) versehen sind!
- Geben Sie Passwörter nie an Dritte weiter! Kein Unternehmen wird Sie dazu auffordern, Ihr Passwort telefonisch oder per E-Mail zu übermitteln!
- Ändern Sie voreingestellte Passwörter (z.B. im WLAN-Router, IoT-Geräten)!
- Notieren Sie Passwörter nicht auf Notizzetteln, die z.B. an Ihrem Bildschirm kleben, oder in unverschlüsselten Textdateien!
- Sollten Sie eine Liste mit Ihren Passwörtern zur Sicherheit anlegen wollen, lagern Sie diese an einem für Dritte unerreichbaren, sicheren Ort, wie z.B. einem Safe
- (Passwörter können auf eigenen Rechnern, die regelmäßig genutzt werden, im Browser und E-Mail-Programmen gespeichert werden) (Zugriff muss durch ein Passwort geschützt sein und Gerät am besten verschlüsselt)
- Sollte Ihr Passwort bekannt geworden sein, ändern Sie es unverzüglich oder lassen Sie Ihren Zugang sperren!

Antivirus-Software und Updates

Da auch Schadsoftware die Sicherheit Ihrer Passwörter und allgemein Ihrer Zugangsdaten gefährden kann, sollten Geräte, auf denen Passwörter eingegeben werden, gegen Schadsoftware abgesichert werden. Auf jeden Fall sollten Sie ein Antivirus-Programm installiert haben. Unter Windows können Sie hierfür den ab Windows 8 standardmäßig mitgelieferten Windows Defender verwenden. Alternativ für Windows, aber auch für MacOS und Linux verfügbar, können Sie sich die Sophos Endpoint Security (https://www.uni-

muenster.de/ZIV/Software/SophosAllgemeineInformationen.html) herunterladen und installieren. Diese wird für Angehörige der Uni Münster kostenfrei bereitgestellt.

Da ein Virenschutzprogramm nicht vor allen Angriffen schützen kann, sollten Sie unbedingt auch darauf achten, regelmäßig Updates (Aktualisierungen), zu installieren. Dies gilt sowohl für das Betriebssystem, als auch für alle installierten Programme. Heutzutage bringen die meisten Programme eigene Aktualisierungskomponenten mit, die automatisch nach Updates suchen und diese auf Wunsch des Nutzers installieren. Auch wenn es manchmal nervig ist und beim Arbeiten mit dem Computer stört, sollten Sie immer zeitnah installiert werden.

Anforderung: Regeln für ein gutes Passwort

Aber auch bei der Wahl des Passworts sollten einige grundlegende Regeln für ein sicheres Passwort beachtet werden, die hauptsächlich gegen Brute-Force-Angriffe schützen:

1. Passwörter sollten mindestens 8 Zeichen lang sein, je länger desto besser (Ausnahme: mindestens 20 Zeichen bei Verschlüsselungsverfahren, wie z.B. WPA2 für WLAN-Zugriffe)
2. Passwörter sollten immer eine Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (?!%+…) sein
3. Passwörter sollten nicht in Wörterbüchern gefunden werden können
4. Ebenso sollten Passwörter nicht einfach Namen von Familienmitgliedern, Freunden oder Lieblingsstars sein
5. Auch andere persönliche Informationen, wie z.B. Geburtsdaten, sind nicht zu empfehlen
6. Passwörter sollten nicht aus Wiederholungs- oder Tastaturmustern bestehen (z.B. 1234abcd, asdfgh, 1111aaaa)
7. Simple Änderungen, wie z.B. das Voranstellen oder Anhängen von einzelnen Ziffern oder Sonderzeichen, sind berechenbar und sollten nicht genutzt werden
8. Auch ein sicheres Passwort hilft nichts, wenn Sie es auf einer Phishing-Seite eingeben, oder wenn der Dienst gehackt wird (siehe https://haveibeenpwned.com/, https://sec.hpi.de/leak-checker/search).

Zwei-Faktor-Authentifizierung

Eine letzte Empfehlung ist die Verwendung von Zwei-Faktor-Authentifizierung. Google, Apple, Microsoft, Dropbox und viele bieten diese Möglichkeit bereits an. Bei der Nutzung von Zwei-Faktor-Authentifizierung werden Sie bei der Anmeldung oder auch nur bei bestimmten Aktionen dazu aufgefordert, eine weitere Information zusätzlich zu Ihrem Passwort einzugeben, um Ihre Identität zu bestätigen. Im Gegensatz zu Passwörtern sind diese Codes immer nur eine sehr kurze Zeitspanne lang gültig und ändern sich danach wieder. Wie Sie diese Codes erhalten, hängt vom Dienst ab. Es gibt verschiedene Möglichkeiten dafür, wobei häufig die Zusendung per SMS oder E-Mail erfolgt, aber auch die Nutzung einer Smartphone-App, die diese Codes generiert, ist möglich. Viele Internetseiten und Dienste bieten mittlerweile Zwei-Faktor-Authentifizierung als optionale Funktion an, z.B. auch unser MeinZIV -Portal. Dieser zusätzliche Schritt kann die Sicherheit Ihrer Zugänge drastisch erhöhen, da Angreifer nun auch den zweiten Faktor erlangen müssten, um Ihre Zugangsdaten zu missbrauchen. Allerdings sollten Sie trotzdem die Empfehlungen zu sicheren Passwörtern und dem Umgang mit ihnen beachten. Die Zwei-Faktor-Authentifizierung soll nur größeren Schaden verhindern, falls tatsächlich mal Ihr Passwort abhandenkommt oder erraten wird.

Lösung/Hilfen/Tipps für die Passworterzeugung

Die Anforderungen an sichere Passwörter sind natürlich schön und gut, aber in der Praxis wenig hilfreich, um neue Passwörter zu erstellen. Aber es gibt einige Tricks mit denen man relativ einfach sichere Passwörter generieren kann und einige Methoden können auch dabei helfen, sich diese zu merken.

Zufällige Passwörter

Die wahrscheinlich beste Methode, um sichere Passwörter zu erzeugen, ist die Nutzung eines Passwortgenerators. Passwortgeneratoren gibt es in verschiedensten Ausführungen, sowohl als Programme, z.B. pwgen (https://www.heise.de/download/product/pwgen-fuer-windows-47128), wie auch als Internetseiten, z.B. der ZIV Passwortgenerator. Nach vorgegebenen Regeln generieren diese zufällige Passwörter von gewünschter Länge.

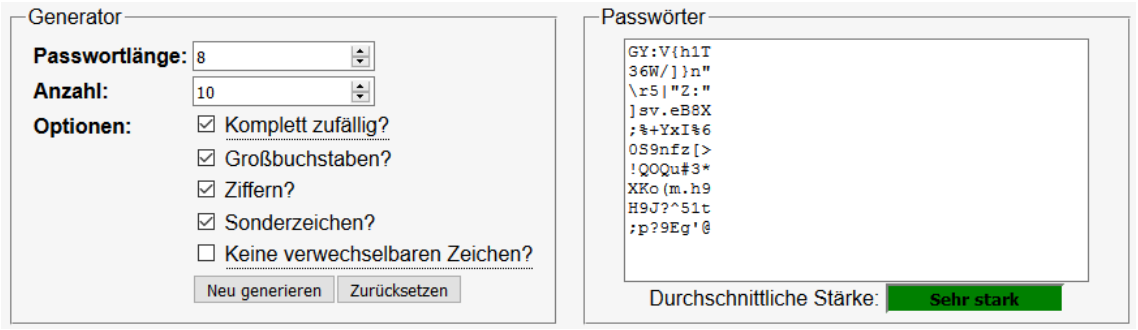


Abbildung 2 - Passwortgenerator des ZIV

Die generierten Passwörter können natürlich sehr komplex werden und hängen vom Zufall ab, weswegen sie sehr sicher gegen Brute-Force-Angriffe sind. Allerdings kann man sie sich kaum merken und einmal vergessen sind diese Passwörter auch nicht wiederherstellbar.

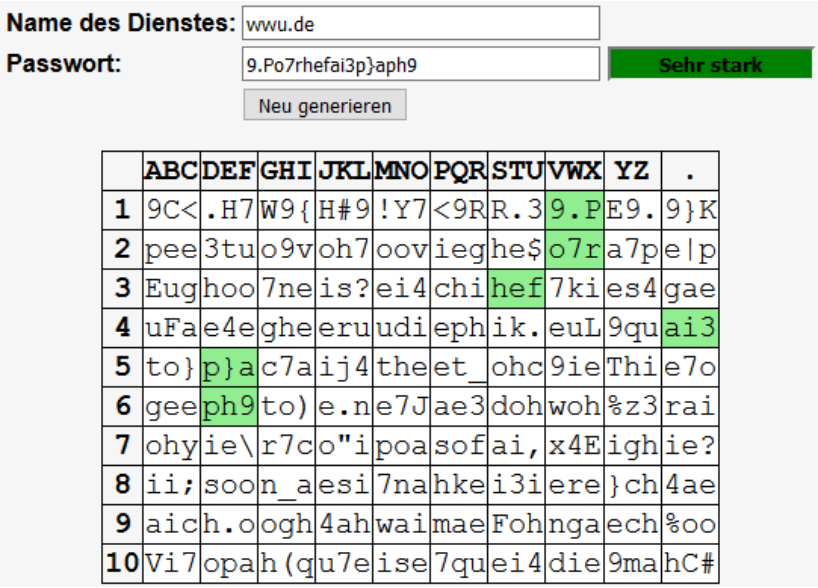
Alternative 1

Eine sehr beliebte und einfache Alternative ist die Merksatzmethode. Hierfür muss man sich zuerst einen Merksatz ausdenken, beispielsweise "Mein Passwort ist > 12 Zeichen und ich benutze es nur für meine E-Mailadresse.". Wichtig ist allerdings, dass der Merksatz selbst gewählt wird und keinesfalls bekannte Zitate oder Redewendungen genutzt werden, denn auch solche Passwörter könnten von Angreifern automatisch generiert und ausprobiert werden. Nun nimmt man von jedem Wort den Anfangsbuchstaben (oder auch immer den 2., 3., oder den letzten), die Ziffern und Sonderzeichen und kombiniert sie zu einem Passwort. Für den Beispielmerksatz könnte das Passwort nun beispielsweise "MPi>12ZuibenfmE-M." lauten. Natürlich können noch weitere Umformungen genutzt werden, wie z.B. das Wort "und" durch "&" ersetzen. Desto kreativer Sie werden und desto zufälliger die Kombinationen sind, desto sicherer kann das Passwort werden.

Mit dieser Methode lassen sich auch komplexere Passwörter leicht merken und können über den Merksatz wiederhergestellt werden. Bei der Nutzung vieler verschiedener Passwörter kann es allerdings schwer werden, alle Merksätze zu behalten und auseinander zu halten.

Alternative 2

Die Nutzung einer Passwortkarte ist eine weitere Möglichkeit, um sich komplexe Passwörter nicht direkt merken zu müssen. Bei der Passwortkarte werden kurze, zufällig generierte Zeichenfolgen auf eine Tabelle verteilt, deren Spalten die Buchstaben des Alphabets und deren Zeilen die Zahlen von 1 bis 10 zugeordnet sind. Man kann nun aus beliebigen Wörtern, z.B. aus dem Namen des Dienstes, für den man das Passwort nutzen möchte, komplexe Passwörter herleiten. Wenn man das unten abgebildete Beispiel nimmt, könnte ein Passwort für "wwu.de" erzeugt werden, indem man zuerst aus der 1. Zeile den Inhalt des Feldes in der Spalte "VWX" nimmt, aus der 2. Zeile den Inhalt des Feldes in der Spalte "VWX", aus der 3. Zeile den Inhalt des Feldes „STU“ und so weiter. Dieses Vorgehen würde das Passwort "9.Po7rhefai3p}aph9" ergeben.



Name des Dienstes: wwu.de

Passwort: 9.Po7rhefai3p}aph9 **Sehr stark**

Neu generieren

	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ	.
1	9C<	.H7	W9{	H#9	!Y7	<9R	R.3	9.P	E9.	9}K
2	pee	3tu	o9v	oh7	oov	ieg	he$	o7r	a7p	e|p
3	Eug	hoo	7ne	is?	ei4	chi	hef	7ki	es4	gae
4	uFa	e4e	ghe	eru	udi	eph	ik.	euL	9qu	ai3
5	to}	p}a	c7a	ij4	the	et_	ohc	9ie	Thi	e7o
6	gee	ph9	to)	e.n	e7J	ae3	doh	woh	%z3	rai
7	ohy	ie\	r7c	o"i	poa	sof	ai,	x4E	igh	ie?
8	ii;	soo	n_a	esi	7na	hke	i3i	ere	}ch	4ae
9	aic	h.o	ogh	4ah	wai	mae	Foh	nga	ech	%oo
10	Vi7	opa	h(q	u7e	ise	7qu	ei4	die	9ma	hC#

Abbildung 3 - Passwortkartengenerator des ZIV

Das Ursprungswort lässt sich leichter merken, als ein gleich komplexes Passwort wie das Resultat. Allerdings benötigt man bei jeder Passworteingabe die Passwortkarte und sollte diese verloren gehen, kann sie nicht mehr wiederhergestellt werden, da die Passwortkarten immer zufällig generiert werden.

Hilfen für Passwortverwaltung

Bei der heutigen Vielzahl an Internetseiten und Diensten können schon eine Menge Zugangsdaten mit Passwörtern zusammenkommen, besonders bei verschiedenen Passwörtern für jeden Dienst. Doch wie kann man all diese Informationen sicher verwalten?

Die sicherste Option ist immer noch Ihr Gedächtnis. Keiner kann Ihre Passwörter von dort entwenden, ganz im Gegensatz zu einem Notizzettel auf Ihrem Schreibtisch oder einer unverschlüsselten Textdatei auf Ihrem Computer. Aber bei zu vielen Passwörtern geht natürlich auch irgendwann der Speicherplatz in Ihrem Kopf zur Neige. Zum Glück gibt es eine Abhilfe, nämlich die Nutzung eines Passwort-Verwaltungsprogramms. Dann müssen Sie sich nur noch ein gutes Passwort ausdenken und merken, mit dem alle anderen Passwörter verschlüsselt abgelegt werden können. Es gibt verschiedene Programme zur Verwaltung von Zugangsdaten, z.B. ist häufig in Ihrem Internet-Browser bereits ein Speicher für Zugangsdaten integriert oder es wird beim Betriebssystem direkt eines mitgeliefert, wie der Schlüsselbund bei Mac OS. Wir möchten Ihnen hier aber ein anderes Programm vorstellen, nämlich Keepass. Welches Programm Sie nutzen, bleibt Ihnen überlassen. Der Vorteil bei Keepass ist die hohe Portabilität und Sicherheit, da Sie die volle Kontrolle über die Passwort-Datei besitzen.

Keepass

Keepass ist ein kostenloses Programm, welches Sie in einer direkt ausführbaren, portablen Version für Windows herunterladen (https://www.heise.de/download/product/keepass-15712) können. Andere Versionen, z.B. für Android, sind von Drittanbietern verfügbar. Nach dem Starten des Programms können Sie eine Passwortdatenbank erstellen, die mit einem Masterpasswort gesichert ist. Anschließend können Sie Ihre Zugangsdaten für verschiedene Dienste eintragen und bei Bedarf nach Kategorien sortieren. Das Programm stellt Ihnen auch weitere Funktionen bereit, wie z.B. die Erzeugung von sicheren, zufällig generierten Passwörtern. Alle eingetragenen Zugangsdaten werden verschlüsselt in einer Datei mit der Endung ".kdbx" abgespeichert. Bei einem guten Masterpasswort ist die Verschlüsselung sicher genug, dass diese Datei auch in Cloud-Speichern (z.B. sciebo) abgelegt werden kann, sodass Sie von überall Zugriff auf Ihre Passwörter erhalten können. Sie sollten allerdings beachten, dass im Falle eines Verlusts der Passwort-Datei oder des Masterpassworts es keine Möglichkeit gibt,

Ihre Passwörter wiederherzustellen. Deswegen sollten Sie unbedingt Sicherungskopien Ihrer Passwort-Datei anlegen und ein Masterpasswort wählen, das Sie sich gut merken können. Sie können zur Sicherheit Ihre Zugangsdaten direkt aus Keepass auch ausdrucken lassen und für den Notfall an einem sicheren Ort, z.B. einem Safe, aufbewahren.

Eine detaillierte Anleitung zur Verwendung von Keepass finden Sie hier: https://www.uni-muenster.de/ZIVwiki/bin/view/Anleitungen/KeePass.

Ansprechpartner/Kontakt

Sollten Sie Fragen oder Probleme haben, können Sie sich an Ihre zuständige IVV (vor allem Mitarbeiter) oder direkt an das ZIV (vor allem Studierende) wenden.

IVVen: https://www.uni-muenster.de/de/zentraledienstleister/ivven.html

ZIV: https://www.uni-muenster.de/ZIV/Hilfe/Ansprechpartner.html

IV-Sicherheit: https://www.uni-muenster.de/IV-Sicherheit