Passwortänderung

Gedanken zum Thema „Passwortsicherheit“
und
Anleitung zum Passwordänderung

zur Verfügung gestellt durch:

ZID – Dezentrale Systeme

Mai 2018

Inhaltsverzeichnis

1. Einleitung zum Thema „Passwortsicherheit“

Das Thema „Passwortsicherheit“ ist sehr aktuell. Angriffe auf User-Passwörter im Bereich Telebanking (das so genannte „Phishing“) sind in den Medien immer wieder präsent.

Immerhin zeigt es sich, dass die Benutzer bei Passwörtern, die vor allem im Bereich „Geld und Internet“ verwendet werden, sehr wohl auf Geheimhaltung und natürlich auch auf Sicherheit bedacht sind.

Weit fahrlässiger ist hingegen der Umgang mit Passwörtern am Arbeitsplatz. Nicht selten findet man hier Post-Its am Monitor, auf denen sämtliche Zugangsdaten zu finden sind. Im Bereich des Arbeitsplatzes sollten keine Passwörter in schriftlicher Form vorhanden sein.

Ein weiteres hohes Sicherheitsrisiko stellt die Weitergabe von Passwörtern an Kollegen oder - noch schlimmer - an Unbefugte dar.

Gerade dies ist am Mozarteum nicht nötig, da jeder Mitarbeiter und auch jeder Student über einen gültigen Account verfügt, mit dem er/sie sich auf den PCs anmelden kann.

Hinweis: Alle personenbezogenen Daten wurden aufgrund der DSGVO unleserlich gemacht.

2. Warum müssen Passwörter geändert werden:

Wird ein Passwort längere Zeit verwendet, so steigt damit die Wahrscheinlichkeit, dass das Passwort (oder Teile davon) anderen Benutzern bekannt wird. Ein

- "über die Schulter gucken" bei der Eingabe des Passwortes,
- das Weitergeben von Passwörtern an Kollegen zur kurzfristigen Benutzung des PCs,
- irrtümliche Eingabe des Passwortes in Klartextfeldern

zählen unter anderen zu den Möglichkeiten, wie ein Passwort im Laufe der Zeit unsicher wird.

Moderne Betriebssysteme bieten die Möglichkeit, den Benutzer nach einer vorgegebenen Zeit automatisch zu der Wahl eines neuen Passwortes aufzufordern. Diese Möglichkeit der Passwortegültigkeit auf eine bestimmte Zeit einzuschränken wird "aging" genannt.

Der wichtigste Schritt bei der Aktivierung des Aging-Verfahrens ist die Aufklärung der Benutzer. Die Benutzer müssen erkennen, dass es sich bei der Aufforderung zum Ändern des Passwortes nicht um eine Schikane des Netzwerkadministrators handelt, sondern dass die Unbedenklichkeit der Passwörter von entscheidender Wichtigkeit ist.

Ein weiteres Problem stellt die Wahl der maximalen Gültigkeitsdauer eines Passwortes dar:

- zu kurze Intervalle dazu führen können, dass sich die Benutzer ein Schema zur Generierung neuer Passworte überlegen (etwa die Verwendung der Monatsnummer bei einem monatlichen Wechsel)
- zu lange Intervalle den Nutzen des Aging nachhaltig beeinflussen.

In diesem Zusammenhang hat es sich bewährt, Passworte mindestens jedes halbe Jahr zu ändern.

Am Mozarteum werden Sie alle 6 Monate – exakt 180 Tage - zum Ändern des Passwortes aufgefordert. Dieser Aufforderung sollten Sie auch umgehend nachkommen, da ansonsten kurze Zeit später Ihr Account gesperrt wird. Nach Ablaufen Ihres Passwortes stehen Ihnen noch 10 so genannte „Grace Logins" zur Verfügung. Mit jedem Anmelden verbrauchen Sie ein solches „Grace Logins".

Sobald Ihr Account gesperrt wurde, ist eine Verbindungsaufnahme mit dem Helpdesk-Team des Zentralen Informatikdienstes (ZID) unumgänglich. Die Mitarbeiter des Helpdesks haben die Möglichkeit, Ihre „Grace Logins" auf 10 Stück zurück zu setzen, so dass Sie noch einmal die Gelegenheit haben, das Passwort zu ändern.

Wesentlich bei der Wahl des Passwortes ist es ein „sicheres" Passwort zu wählen. Was zeichnet nun ein „sicheres" Passwort aus? Was ist sonst noch bei der Wahl des Passwortes zu beachten? Auf diese Fragen soll im folgenden Kapitel eingegangen werden.

3. Das „sichere" Passwort:

Die Wahl eines "sicheren" Passwortes ist entscheidend. Da dem Benutzer bei der Wahl eines Passwortes große Verantwortung übertragen wird, ist eine umfassende Aufklärung der Benutzer zu diesem Thema wichtig.

Bei der Auswahl eines Passwortes sollte darauf geachtet werden, dass dieses nicht leicht zu erraten ist. Problematisch sind dabei alle Passworte, die von einem Angreifer ausprobiert werden, z. B.:

- Worte aus dem Sprachschatz (div. Wörterbücher)
- Worte aus anderen Sprachen (ebenfalls div. Wörterbücher)
- alle Arten von Namen (Personen, Städte, Gebäude, Comic-Figuren, ...)
- Rechnernamen, Benutzerkennungen
- Geburtsdaten, Telefonnummern, PIN-Codes
- Abkürzungen
- Tastaturfolgen (z.B. "QWERTZ" oder "ASDFGH")
- Anfangsbuchstaben von bekannten Sprichwörtern, Liedern, etc. (z. B. amesads = "alle meine Entchen schwimmen auf dem See", ...)
- etc.

Ebenso unbrauchbar sind Modifikationen dieser Worte durch z.B.:

- Rückwärtsschreibung (retep, reteP, ...)
- Anhängen oder Voranstellen einer Zahl (peter09, 7peter, ...)
- Anhängen oder Voranstellen eines beliebigen Zeichens (peter$, %peter, ...)
- etc.

In diesem Zusammenhang ist vom Verwenden von Umlauten (ä, ö, ü) und von Sonderzeichen (§, $, %, &t, /, *, +, #, =, ...) in Passwörtern eher abzuraten. Gerade beim Gebrauch von fremdsprachiger/-n Software/Clients kann es zu erheblichen Schwierigkeiten kommen.

3.1. Was müssen Sie bezüglich Passwörter am Mozarteum noch beachten?

- Das System merkt sich die von Ihnen zuletzt verwendeten Passwörter (50 Stück). Sie können somit diese Passwörter nicht mehr verwenden. Ein zuvor in Kleinbuchstaben und nun in Großbuchstaben geschriebenes Passwort wird als das gleiche erkannt.

- Das gewählte Passwort muss mindestens eine Länge von 8 Zeichen haben. Je länger ein Passwort ist, desto schwieriger ist es, dass dieses von Unbefugten missbraucht werden kann.

3.2. Wie sollen sich nun diese acht Zeichen zusammensetzen, damit sie ein „sicheres" Passwort ergeben?

Am Mozarteum sollten mindestens zwei Ziffern/Zahlen in Ihrem Passwort enthalten sein. Die restlichen Zeichen sollten einen „Buchstabensalat" ergeben, den Sie durch das Mischen von Groß- und Kleinbuchstaben noch variieren können.

Konkret könnte somit ein Passwort wie folgt aussehen:

- aWdFRg47 oder
- LLh63bFc oder
- 91mbAYsq oder
- etc.

Solche Zeichenfolgen sind natürlich schwer zu merken. Allerdings steht unbestritten fest: Je schwerer das Passwort zu merken ist, desto schwieriger ist das Erraten des Passwortes. Und gerade das ist ja das erklärte Ziel dieses Papers!

3.3. Passwort-Richtlinien am Mozarteum

Das Passwort sollte idealer Weise mindestens 2 Buchstaben, 2 Ziffern und 1 Sonderzeichen beinhalten.

- Die Groß- und Kleinschreibung des Passworts muss berücksichtigt werden.
- Muss mindestens 8 Zeichen lang sein.
- Darf keinen der folgenden Werte enthalten: password test 123456789 12345678 qwertzui
- Darf keinen Teil Ihres Namens oder Benutzernamens enthalten.
- Darf kein häufiges Wort und keine häufig verwendete Zeichenfolge enthalten.
- Das neue Passwort darf nicht zuvor verwendet worden sein.

4. Zusammenfassung:

Passwörter schützen den Benutzer und dessen Dateien vor unbefugtem Zugriff anderer. Deshalb ist es wichtig, dass der grundsätzliche Charakter eines Passwortes – geheim zu sein – nicht verloren geht.

Zum Erraten von Passwörtern durch Angreifer werden große Wortlisten benutzt. Die darin enthaltenen Worte stammen aus diversen Wörterbüchern, Sammlungen von Namen, Abkürzungen etc.

Ein Passwort, das

- von einem Wort aus einem Sprachschatz (auch aus anderen Sprachen),
- einen Name,
- einer Abkürzung oder
- einer Tastaturfolge (wie z.B. "QWERTZ") abstammt,

ist als Passwort ungeeignet. Auch Modifikationen von solchen Worten sind als Passwörter nicht zu empfehlen.

Das Aging-Verfahren kann nur dann funktionieren, wenn User in regelmäßigen Abständen Ihr Passwort ändern und dieses auch geheim halten.

(1) Passwörter sollten am Mozarteum sofort bei Aufforderung geändert werden. Bei Schwierigkeiten kontaktieren Sie das Helpdesk-Team des ZIDs.

(2) Passwörter sollten eine Länge von 8 Zeichen haben; davon mindestens 2 Ziffern. Variieren Sie zwischen Groß- und Kleinschreibung.

(3) Je komplizierter die Zeichenfolge, desto schwieriger das Erraten des Passwortes!

5. Passwortänderung im Micro Focus GroupWise Webaccess

Gerade für Benutzer, denen kein PC zur Verfügung steht, beziehungsweise die Ihre PC-Arbeit – Bearbeiten der Emails, Internetrecherchen, etc. – von zu Hause aus erledigen wollen, ist es wichtig, dass es eine Möglichkeit gibt, das Passwort ändern zu können. Dies wird mit Novell Webaccess ermöglicht.

Vor- und Nachteile:

- Sie können von zu Hause aus das Passwort wechseln
- Sie benötigen einen Internetzugang.
- Sie benötigen einen Browser; die Sicherheitsstufe sollte auf „Mittel" gestellt sein.
- Sie müssen Micro Focus GroupWise Webaccess einsetzen.

Die Auswirkungen, wenn das Passwort nicht rechtzeitig geändert wurde, sollten mittlerweile bekannt sein: Verbrauchen der „Grace Logins" und in weiterer Folge Aussperren aus dem System.

Ab diesem Zeitpunkt ist eine Verbindungsaufnahme mit dem Helpdesk-Team unumgänglich. Dieses kann die abgelaufenen „Grace Logins" noch einmal zurücksetzen

Zum Ändern des Passwortes mittels Micro Focus GroupWise Webaccess gehen Sie wie folgt vor: Stellen Sie eine Verbindung zum Internet her. Öffnen Sie Ihren Webbrowser (vorzugsweise Mozilla Firefox).

Sie haben nun folgende Varianten:

(1) über die Homepage des Mozarteums: http://www.moz.ac.at bzw. http://www.uni-mozarteum.at rechts oben „Login" wählen und auf der folgenden Seite wählen Sie zwischen „GroupWise – 1. Mailserver" und „GroupWise – 2. Mailserver"

(2) direkt über die Internetadresse: https://webaccess.moz.ac.at/gw/webacc bzw. alternativ dazu die Adresse https://webaccess.**2nd**.moz.ac.at/gw/webacc

Mit beiden Möglichkeiten gelangen Sie zu Abbildung 1:

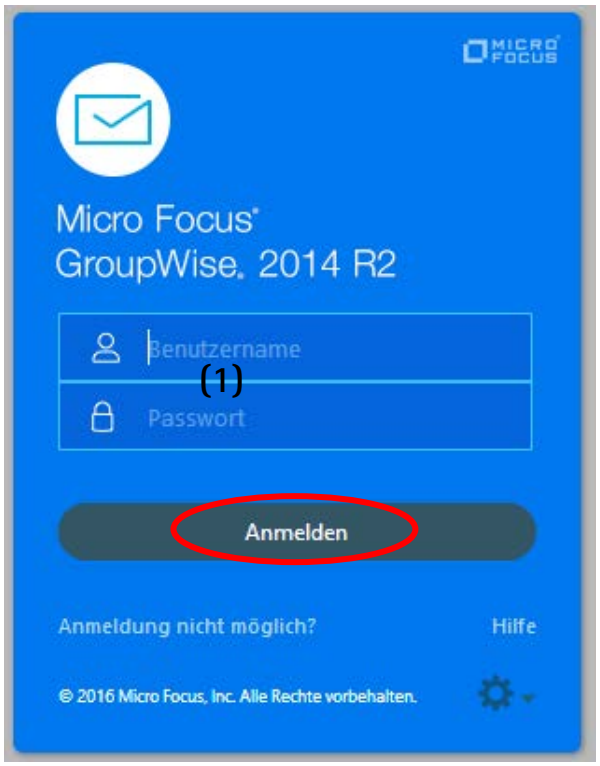

Abbildung 1

(1) In das Feld „Benutzername" geben Sie Ihren Benutzernamen ein. Im Feld „Passwort" geben Sie Ihr aktuelles Passwort ein. Klicken Sie dann mit der linken Maustaste auf „Anmelden" (rot eingekreist).

In weiterer Folge sollten Sie die unten angeführte Abbildung 2 sehen.

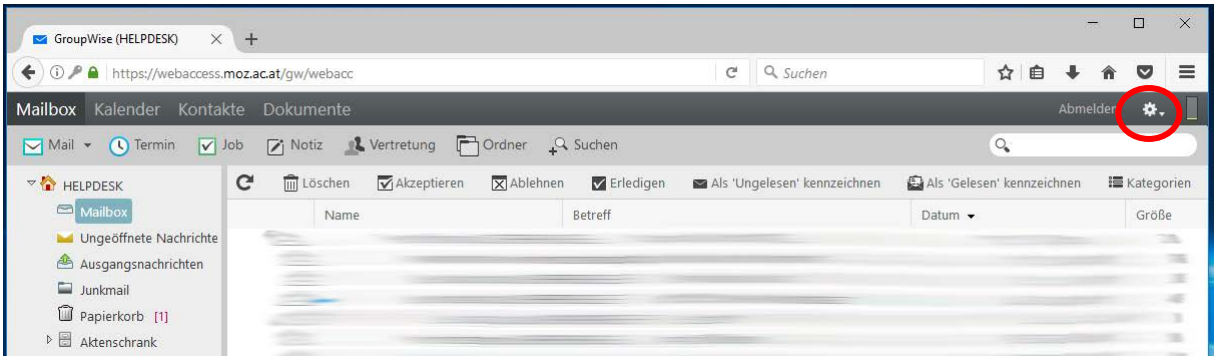

Abbildung 2

Klicken Sie mit der linken Maustaste auf das „Zahnrad"-Symbol (Abbildung 2, rot eingekreist). Wählen Sie den Menüeintrag „Optionen" aus. Es erscheint ein neues Fenster (Abbildung 3). Klicken Sie in dem neuen Fenster auf die Registerkarte „Passwort" (Abbildung 3, rot eingekreist).

Abbildung 3

Sie sollten dann folgende Darstellung sehen:

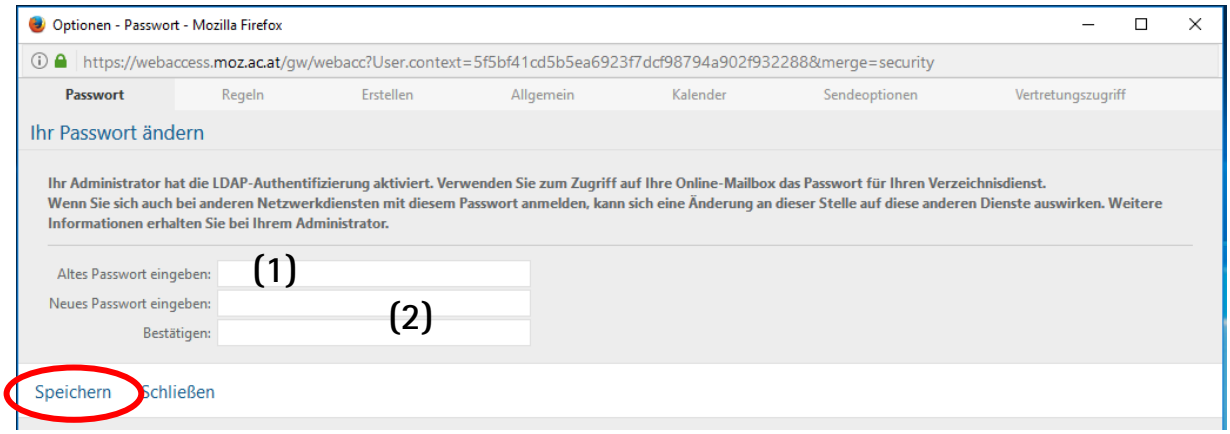

Abbildung 4

(1) Geben Sie im Eingabefeld „Altes Passwort eingeben" Ihr **aktuelles** Passwort ein. Springen Sie dann mit der Tabulatortaste oder klicken Sie mit der linken Maustaste in die nächste Zeile.

(2) Geben Sie im Feld „Neues Passwort eingeben" Ihr **neues** Passwort ein. Gehen Sie in die letzte Zeile „Bestätigen" und wiederholen Sie dort Ihr neues Passwort. Klicken Sie daraufhin mit der linken Maustaste auf „Speichern" (Abbildung 4, rot eingekreist). Danach sollten Sie Abbildung 5 sehen.

In der linken unteren Ecke erscheint „Passwort gespeichert". Klicken Sie zum Abschluss noch auf „Schließen".

6. Passwortänderung im Micro Focus GroupWise

Die Änderung des Passwortes ist auch im GroupWise Client möglich. Klicken Sie in der Menüleiste auf „Werkzeuge“ und dann auf „Optionen“ (Abbildung 6, rot eingekreist).

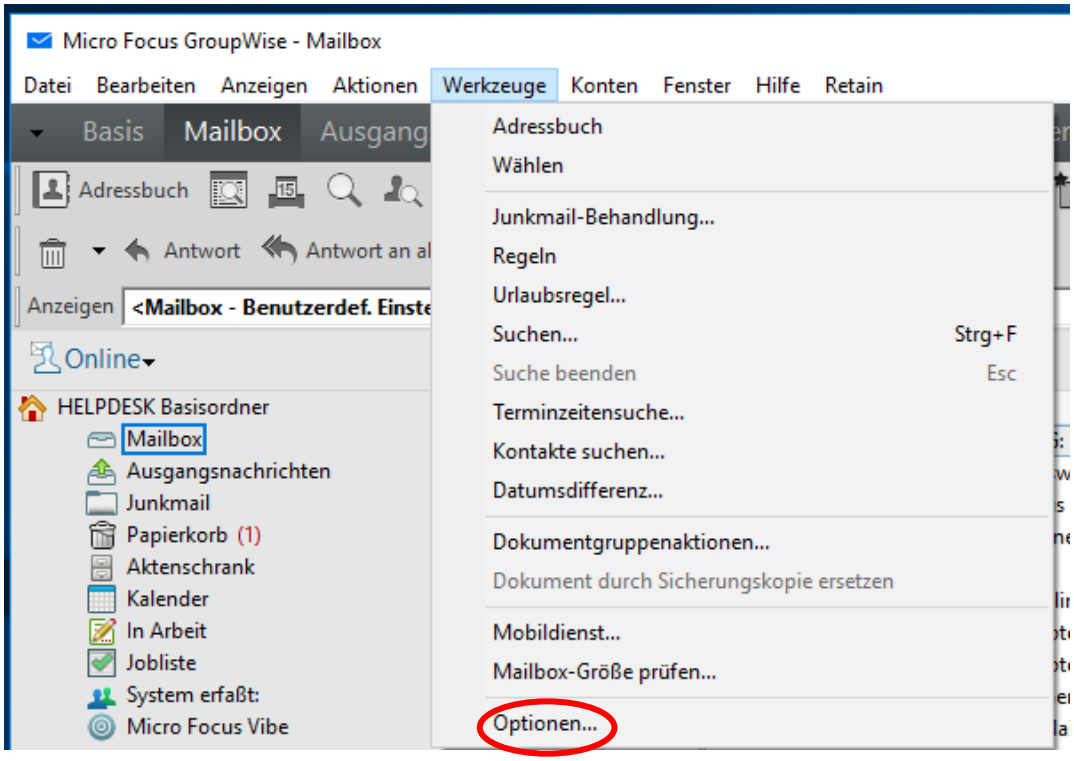

Abbildung 5

Im nächsten Fenster machen Sie einen Doppelklick auf „Sicherheit“ (Abbildung 7, rot eingekreist).

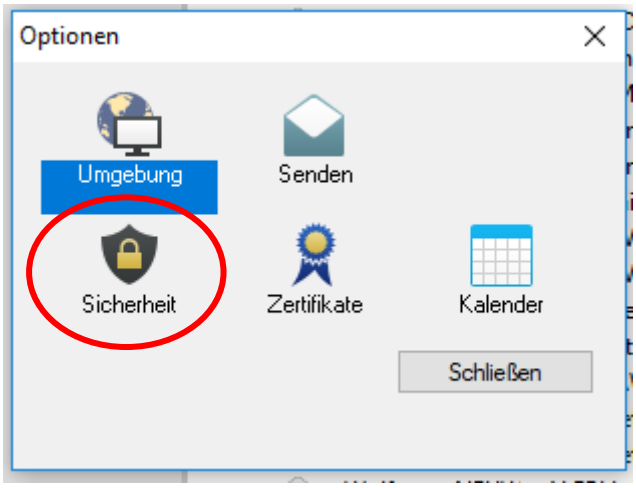

Abbildung 6

Im Fenster „Sicherheitsoptionen“ (siehe Abbildung 8) können Sie nun das Passwort ändern. Bevor Sie irgendwelche Einträge in diesem Fenster machen, werden Sie feststellen, dass die

Eingabefelder „Neues Passwort“ **(2)** und „Neues Passwort bestätigen“ **(3)** zu diesem Zeitpunkt „ausgegraut“ sind.

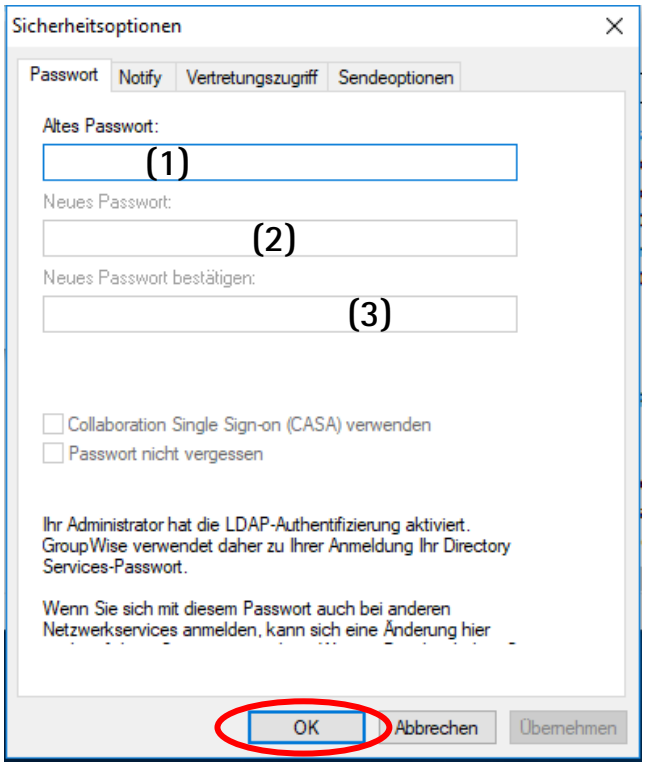

Abbildung 7

Geben Sie im Eingabefeld „Altes Passwort“ **(1)** Ihr aktuelles Passwort ein. Wenn Sie nun mit der Tabulatortaste in das nächste Eingabefeld springen bzw. mit der linken Maustaste in das nächste Feld klicken, können Sie die weiteren Eingabefelder befüllen. Geben Sie das neue Passwort sowohl in die Eingabefelder „Neues Passwort“ **(2)** und „Neues Passwort bestätigen“ **(3)** ein. Klicken Sie auf „OK“ (Abbildung 8, rot eingekreist).

Klicken Sie zum Abschluss im „Optionen“-Fenster (Abbildung 7) auf „Schließen“.

7. Passwortänderung mittels „Strg-Alt-Entf“

Sie können die Passwortänderung auch mittels der Tastenkombination „Strg-Alt-Entf“ auf einem Rechner am Mozarteum durchführen. Diese Art der Passwortänderung ist von zu Hause aus nicht möglich! Wenn Sie den Desktop sehen, drücken Sie gleichzeitig die Tasten „Strg“, „Alt“ und „Entf“. In der neuen Ansicht wählen Sie „Kennwort ändern…“ (Abbildung 8, rot eingekreist) aus.

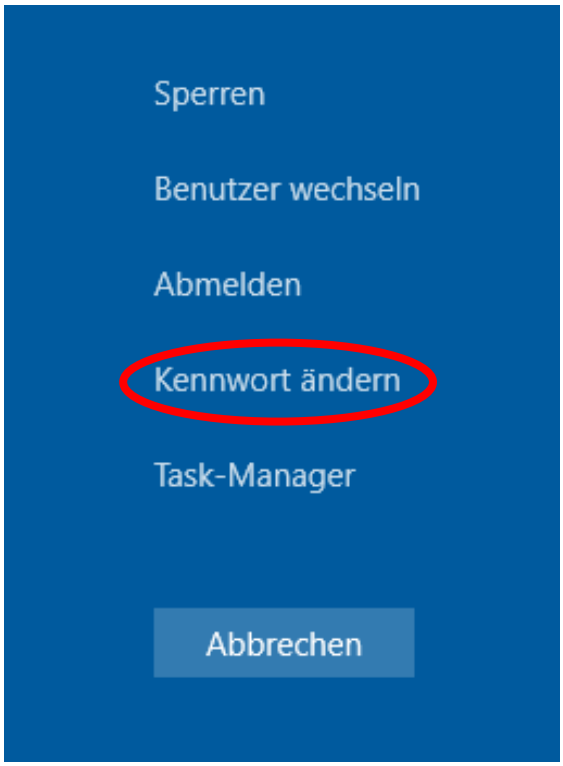

Abbildung 8

Es erscheint die „Netzwerkpasswort ändern" – Ansicht (Abbildung 9).

Abbildung 9

(1) Im ersten Eingabefeld ist der Benutzername des jeweiligen Accounts eingetragen, in diesem Beispiel „helpdesk". Genau für diesen Account wird in weiterer Folge das Passwort geändert.

(2) Im zweiten Feld „Altes Passwort" geben Sie das aktuelle Passwort ein.

(3) Im dritten Feld „Neues Passwort" geben Sie das neue Passwort ein.

(4) Im vierten Feld („Neues Passwort bestätigen") geben sie zur Kontrolle das neue Passwort noch einmal ein

(5) Klicken Sie dann auf den „Pfeil"-Button (Abbildung 9, rot eingekreist).

Im Anschluss erfolgt eine Anzeige (Abbildung 10), in welcher zu beachten ist, dass beide Instanzen (sowohl der Name des PCs als auch MOZ blau markiert sind). Ist dies der Fall kann mit Klick auf „OK" das Passwort übernommen werden.

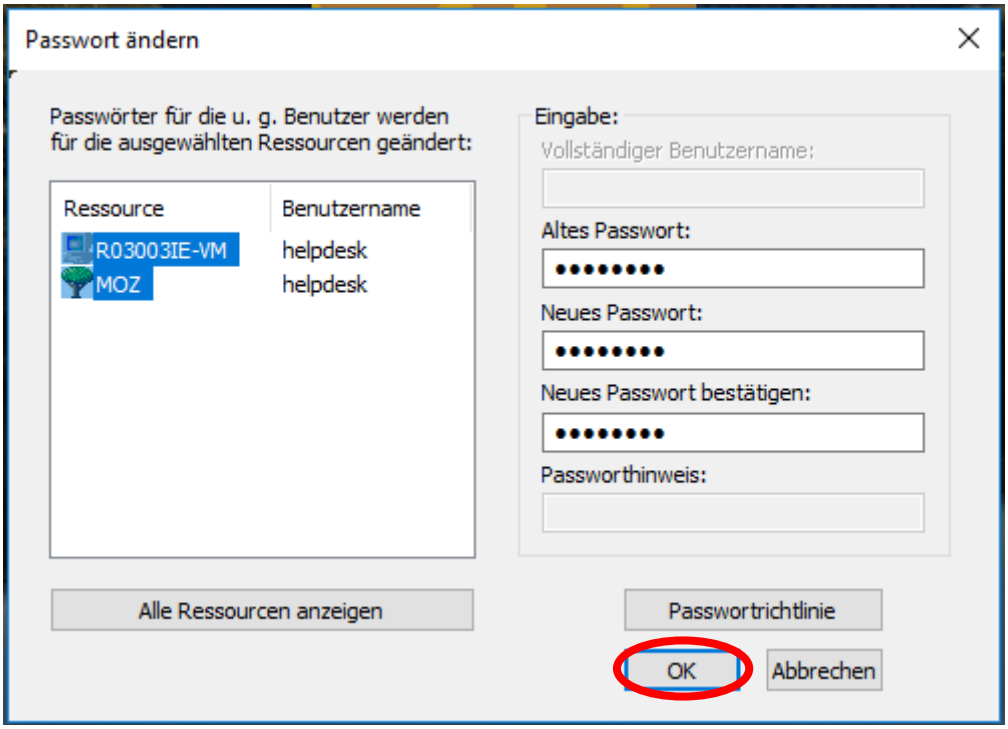

Abbildung 10

8. Passwortänderung mittels Self Service Password Reset

Des weiteren kann das Passwort auch mittels dem Self Service Password Reset geändert werden. Die erste Voraussetzung um diesen Dienst nutzen zu können, ist das Speichern einer privaten Mail-Adresse beim erstmaligen Einstieg in dieses System, damit künftig die Passwortänderung dort erfolgen kann. Diese E-Mail-Adresse wird von der Universität Mozarteum zu keinem anderen Zweck verwendet.

Der Zugang zum Self Service Passwort Reset ist möglich über die Homepage der Universität Mozarteum Salzburg – http://www.uni-mozarteum.at. Über „Login" (rechts oben auf der Startseite) kommen Sie zu dem Link für „Self Service Passswort Reset". Sie können aber auch direkt über die Webadresse https://sspr.moz.ac.at/sspr/private/Login dorthin gelangen.

Mit beiden Möglichkeiten gelangen Sie zur Abbildung 11:

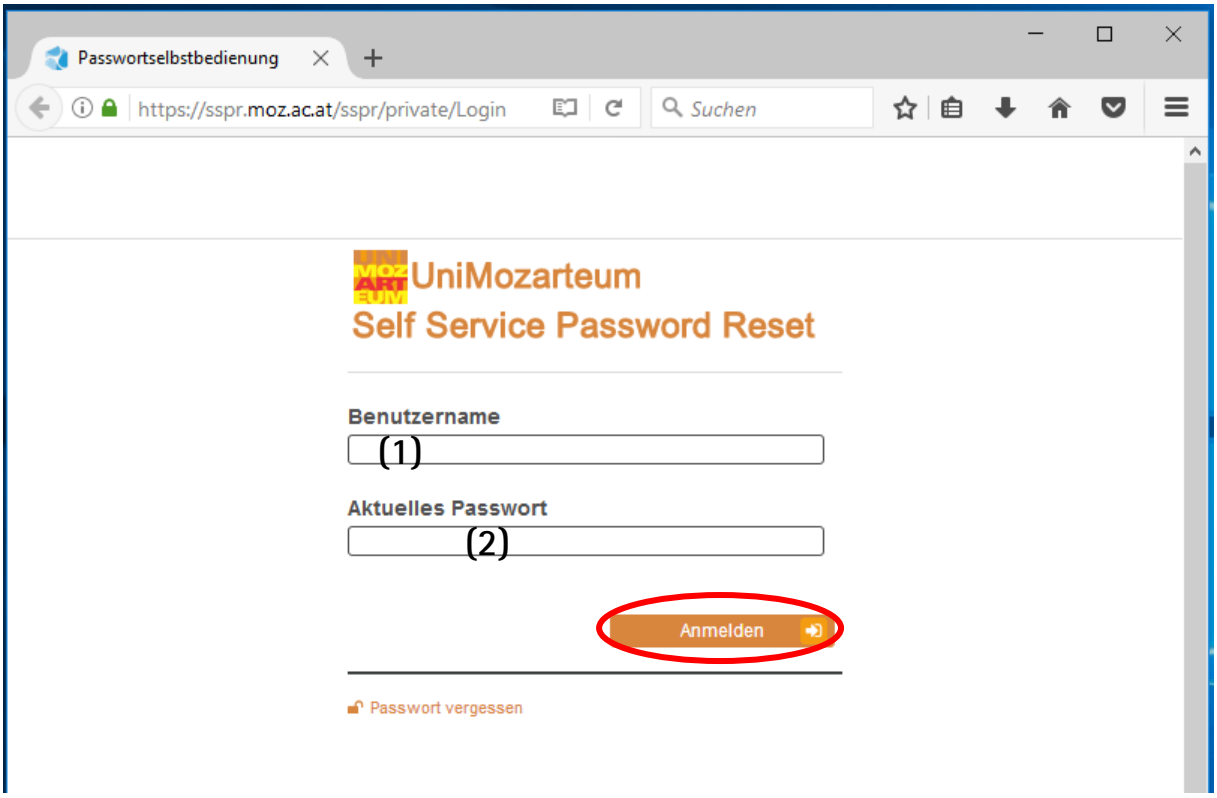

Abbildung 11

(1) In das Feld „Benutzername" geben Sie Ihren Benutzernamen ein. Springen Sie mit der Tabulatortaste oder klicken Sie mit der linken Maustaste in die zweite Zeile

(2) Im Feld „Passwort" geben Sie Ihr aktuelles Passwort ein. Klicken Sie mit der linken Maustaste auf „Anmelden" (rot eingekreist).

Sollten Sie noch keine private E-Mail-Adresse hinterlegt haben, wird Ihnen die unten angeführte Abbildung 12 angezeigt. Bitte in den entsprechenden Feldern die private E-Mail-Adresse hinterlegen und auf „Aktualisieren" klicken. (rot eingekreist).

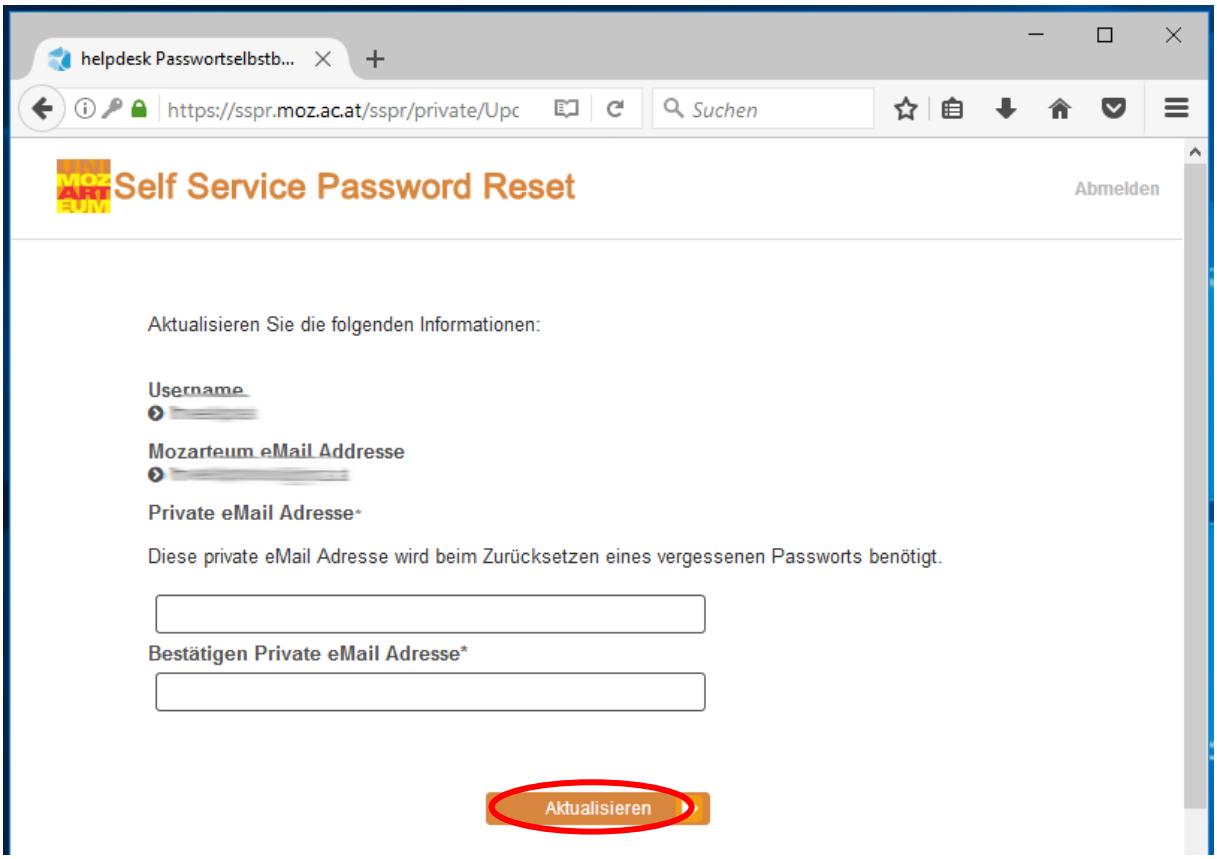

Abbildung 12

Diese E-Mail-Adresse wird von der Universität Mozarteum zu keinem anderen Zweck verwendet.

In weiterer Folge sollten Sie die unten angeführte Abbildung 13 sehen.

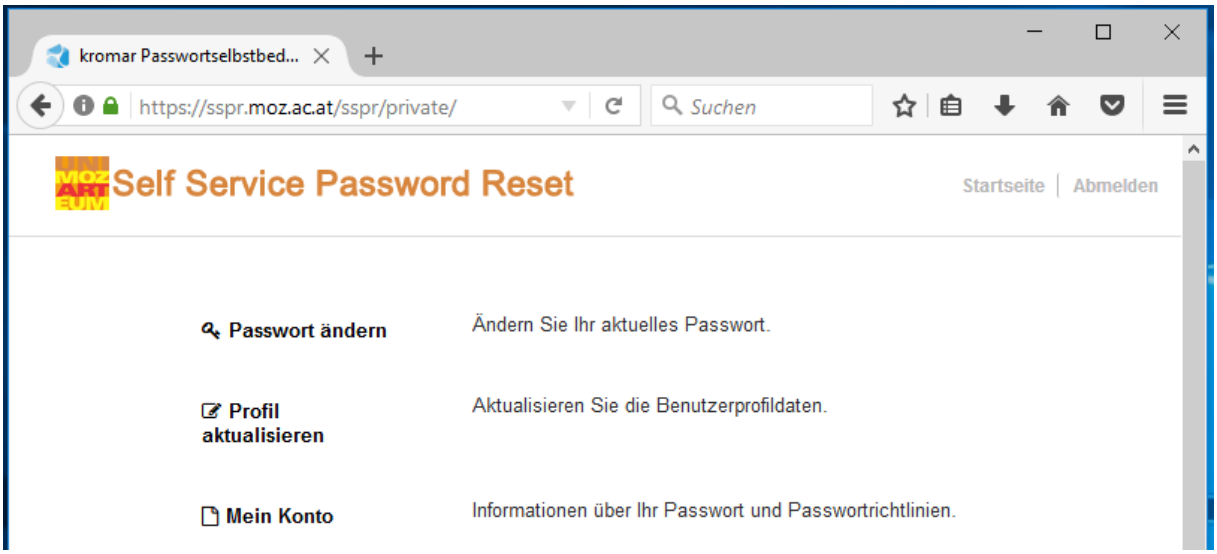

Abbildung 13

In diesem Bereich können Sie das Passwort ändern, Ihre Benutzerprofildaten bearbeiten oder einsehen, wie lang Ihr Passwort gültig ist.