medo.check®
Health and Fitness
Software Solutions

Hinweise zum Umgang mit Antivirus-Produkten

Über dieses Dokument

Dieses Dokument informiert Sie über Einstellungen und Ausnahmen im Zusammenhang mit Antivirus-, Systemoptimierungs- und ähnlichen Softwarelösungen. Diese Einstellungen sind beim Betrieb Ihrer medo.check®-Software notwendig, oder sorgen für eine bessere Performance.

Bei der medo.check®-Software handelt es sich um eine branchenspezifische Software. Das bedeutet, dass es sich zwangsläufig um eine im Vergleich mit anderen Anwendungen selten anzutreffende Software handelt. Für Antivirus-Lösungen ist dies ein besonderes Kriterium, da alle modernen Antivirus-Lösungen immer weniger nach bekannten Bedrohungen, als vielmehr nach neuen, bis dahin unbekannten Programmen suchen, bei denen es sich potenziell um Bedrohungen, also Schadsoftware handeln *könnte*. Die Antivirus-Lösung versucht dann, das Gefahrenpotenzial einer solchen, unbekannten Software abzuschätzen. Ein Prozess, der naturgemäß sogar relativ häufig zu falschen Einschätzungen führt.

Wir möchten Sie mit diesem Dokument daher über ratsame Einstellungen informieren, die Ihre Arbeit und ihre grundsätzliche Zufriedenheit mit der medo.check® Software verbessern, Sie aber auch vor einem Datenverlust durch „übereifrige“ Antivirus-Produkte schützen können.

In Windows 10 Installationen ist grundsätzlich immer auch eine Antivirus-Lösung vorhanden. Wenn kein anderes Produkt diese Funktion übernimmt, ist der zum Betriebssystem gehörige Microsoft Defender aktiv. **Sie sollten sich daher mit den folgenden Hinweisen auseinandersetzen, auch wenn Sie der Meinung sind, gar keine Antivirus-Lösung zu verwenden.**

medo.check®

Health and Fitness
Software Solutions

Empfohlene Ausnahmen

Wir empfehlen, folgende Ordner komplett von Antivirus-Scans auszuschließen, und zwar sowohl vor sogenannten „Life-Scans“, die spontan beim Zugriff auf die Datei stattfinden, wie auch vor turnusgemäßen Komplett-Scans, die z.B. wöchentlich stattfinden, wenn der Rechner gerade nicht benutzt wird.

Ziehen Sie bitte Ihren IT-Dienstleister zu Rate, wenn Sie nicht wissen, wie diese Ausnahmen bei Ihrem Antivirus-Produkt vorgenommen werden.

Falls Sie bei der Installation andere Datei-Ablageorte gewählt haben, als von uns vorgeschlagen: Fügen Sie dann bitte die von Ihnen gewählten Datei-Ablageorte den Antivirus-Ausnahmen hinzu.

- **medo.check Programmdateien:**

  C:\Programme (x86)\medo.check bzw. C:\Program Files (x86)\medo.check

- **medo.check (Kunden-)Daten und Einstellungen**

  C:\ProgramData\medo.check
  Das Verzeichnis C:\ProgramData ist ein von Windows bereitgestellter Ordner, der versteckt angelegt wird. Es kann daher notwendig sein, den Ordnernamen von Hand einzugeben.

Zusätzlich sollten **Nutzer der medo.check Cloud Services** folgende Ordner vor dem Zugriff von Antivirus-Lösungen sperren:

- **OpenVPN:**

  C:\Program Files\OpenVPN bzw. C:\Programme\OpenVPN

- **NSSM-Dienst:**

  C:\Program Files\NSSM bzw. C:\Programme\NSSM

Wenn Sie mehrere **vernetzte Arbeitsplätze** verwenden, ist es unbedingt ratsam, den **Speicherort der Datenbank und die Programmdateien der Datenbank** zu schützen:

- Falls ein **MySQL-Server** installiert wurde:

  C:\Program Files\MySQL\MySQL Server 5.7 bzw. C:\Programme\MySQL\MySQL Server 5.7
  und der Datenordner:
  C:\ProgramData\MySQL\MySQL Server 5.7

- **Andere Datenbanksysteme**: Fügen Sie sowohl den Ablageort für Programmdateien hinzu sowie unbedingt auch den Ablageort der Daten selbst.

Empfohlene Einstellungen

Wir empfehlen, grundsätzlich die Einstellungen der Antivirus-Lösung derart zu treffen, dass ein Eingreifen der Antivirus-Lösung dem Benutzer auch angezeigt wird. Nur so lässt sich für Sie ein Zusammenhang zwischen dem Ausbleiben einer Programmfunktion oder auch einem „Absturz“ und einem Eingriff der Antivirus-Software herstellen.

Die Suche nach unbekannten Dateien wird meist als „Heuristik-Suche“ bezeichnet. Das bezeichnet also die Viren-Suche aufgrund von bloßen Vermutungen oder Verdachtsmomenten. Hier kann schon der Umgang mit PDF-Dateien dafür sorgen, dass medo.check® als gefährlich eingestuft wird. Sorgen Sie daher unbedingt für die oben beschriebenen Ausnahmen.

Damit bei einem fälschlichen Eingreifen der Antivirus-Lösung keine Daten verlorengehen, sollten Sie insbesondere darauf achten, dass auch große Dateien zunächst in den Quarantäneordner verschoben werden. Manche Antivirus-Lösungen sichern nur recht kleine Dateien. Ihre Kundendatenbank kann leicht einige Gigabyte an Umfang haben und würde dann ggf. vom Antivirus gelöscht **– das Ende Ihrer Daten**, wenn Sie keine Datensicherung gemacht haben!

Unbrauchbare Antivirus-Lösungen

Einige wenige Antivirus-Lösungen lassen es nicht zu, einen ganzen Ordner – wie oben beschrieben – von der Überwachung auszuschließen. Bei diesen Lösungen müssten mindestens alle Programmdateien aber zur Vorsicht auch alle Datendateien einzeln als Ausnahme erfasst werden. Nach jedem Update müsste der Schutz auf neu hinzugekommene Dateien ausgedehnt werden. Dieser Aufwand (nach aktuellem Stand über 220 Programmdateien für eine einfache medo.check® Installation) ist wirtschaftlich kaum zu rechtfertigen. Wählen Sie in einer solchen Situation eine andere Antivirus-Lösung.

Falls Ihr Antivirus bereits irrtümlich aktiv wurde…

Grundsätzlich können Sie sich in einer solchen Situation an den medo.check® Support wenden. Es besteht aber die Möglichkeit, dass Ihre Kundendaten durch den Eingriff der Antivirus-Lösung bereits beschädigt wurden. In einigen Fällen lassen sich Dateien aus der sogenannten „Quarantäne“ oder „Isolierung“ wiederherstellen. Das gelingt aber nicht immer, insbesondere wenn sich der Antivirus im Falle großer Datenbankdateien für eine sofortige Löschung entschieden hat.

Wir müssen uns leider vorbehalten, eine solche Hilfeleistung nach geltenden AGB in Rechnung zu stellen, insbesondere dann, wenn der Aufwand einer Datenrettung größer ist, als das Zurückspielen einer Datensicherung.

Bitte beachten Sie die Backup-Empfehlungen im Service-Bereich von medocheck.de und sichern Sie regelmäßig Ihre Daten!

Firewall-Funktionen

Viele Antivirus-Lösungen beinhalten auch eine sogenannte Firewall. Es handelt sich dabei um Techniken, die Programmen den Empfang oder das Senden von Daten verbieten können.

Ihre medo.check® Software benötigt für folgende Funktionen eine Internetverbindung:

- Aktivierung der Lizenz
  Spätestens alle 30 Tage wird Ihre Lizenz online überprüft. 10 Tage vor Ablauf der aktuellen Aktivierung erhalten Sie einen Hinweis darauf, dass sie bald online gehen müssen.
- Updates
  Sie erhalten nach der ersten Anmeldung einen Hinweis, wenn eine neuere medo.check®-Version vorliegt. Um nachzuschauen, ob das der Fall ist, müssen Sie online sein. Fehlt die Online-Verbindung, erhalten Sie keine Update-Hinweise.
- medo.coach®
  Um Trainingspläne und Dokumente an die App zu senden oder Trainingsfeedbacks zu empfangen, wird ein Internetzugang benötigt. Auch der Austausch per Chat findet nur online statt.
- Onlinebuchungstool
  Der Austausch zwischen medo.check® und dem Onlinebuchungstool bewahrt Sie vor Doppelbuchungen.

Ausnahmen beim Download von Dateien

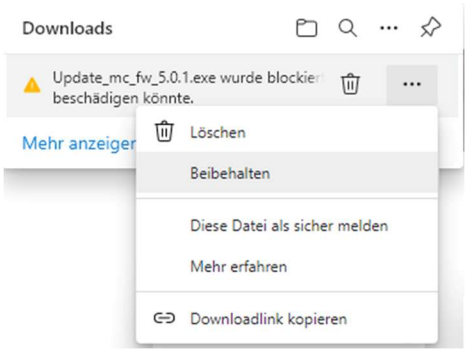
Seit kurzem werden Sie beim Herunterladen von seltener Software bereits beim Download „geschützt“. Dieser Schutz suggeriert bereits ein hohes Gefahrenpotenzial. Derzeit findet dieser Schutz auf zwei Ebenen statt, nämlich im Browser und beim ersten Ausführen einer Datei aus dem Internet. Als medo.check®-Anwender sehen Sie solche Meldungen möglicherweise bei der Installation oder wenn Sie ein Update manuell herunterladen.

Schutzfunktionen des Browsers (Microsoft Edge)

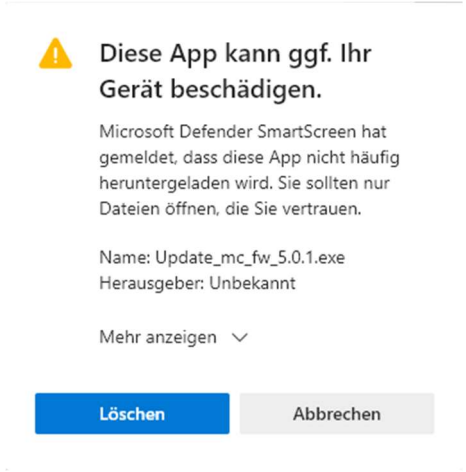
Nach derzeitigem Stand warnt Sie vor allem Microsoft Edge davor, dass Sie eine unbekannte Datei heruntergeladen haben.

Beim Download erscheint zunächst ein Warndreieck am Download-Symbol:

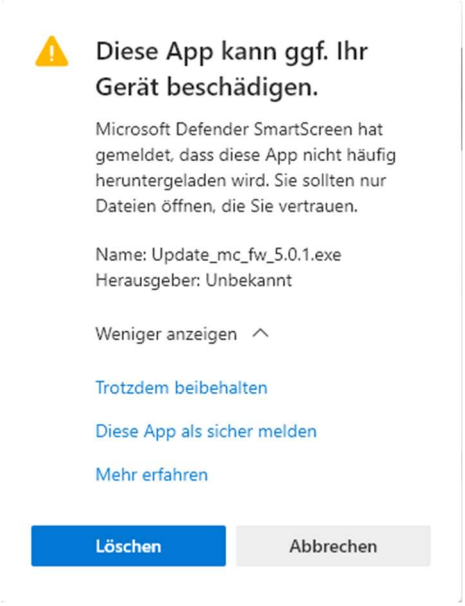
Lässt man die Downloads anzeigen, sieht man eine Warnmeldung und muss über das „…“-Menü den Wunsch äußern, die Datei beizubehalten:



Der Klick auf „Beibehalten“ genügt dem Browser jedoch nicht. Es wird noch einmal nachgefragt:



Auch hier ist die Option „**Trotzdem beibehalten**“ zunächst vor Ihnen verborgen und muss über einen Klick auf „Mehr anzeigen“ sichtbar gemacht werden:



Erst nach dem Klick auf „Trotzdem beibehalten“ kann man die Datei ausführen.

Schutzfunktion von Windows 10

Windows warnt ebenfalls beim Ausführen seltener Dateien:

Erst mit einem Klick auf „Weitere Informationen“ wird die benötigte Option sichtbar:

Nun kann „Trotzdem ausführen“ gewählt werden.