

Unverzichtbare Vorsichtsmaßnahmen: Datensicherung und Antivirus-Ausnahmen

Seit geraumer Zeit weisen wir regelmäßig darauf hin, doch es ist immer wieder zu beklagen, dass Kunden Ihre Daten verloren haben, da sie weder eine regelmäßige Sicherung noch die von uns dringendst empfohlenen Antivirus-Ausnahmen konfiguriert haben.

Die Situation ist sehr leicht beschrieben:

- Ihre Antivirus-Lösung findet eine seltene Anwendung auf Ihrem Gerät vor: medo.check ist wie **alle branchenspezifischen Lösungen** weit weniger häufig anzutreffen, als ein Browser, ein Grafik- oder ein Textprogramm. Die Vermutung, dass dies auch für sich selbst massenhaft verbreitende Schadsoftware gilt, ist sicherlich diskutierbar.
- Die Antivirus-Lösung entschließt sich im Einzelfall, eine seltene Datei als „gefährlich“ einzustufen. Das nennt sich „**heuristische Suche**“, also eine **Einschätzung aufgrund bloßer Vermutungen**.
- Ihre Antivirus-Lösung will die vermeintliche Gefahr von Ihrem Gerät bannen: Die „vermutlich gefährliche Datei“ wird unter Quarantäne gestellt, und sicherheitshalber alle Dateien, die von der „vermutlich gefährlichen“ Datei verändert wurden. Sie ahnen es: Das sind **ihre Kundendaten**.
- Ihre Kundendatenbank ist aber einige hundert Megabyte groß – das ist ganz normal, da allein aufgrund der gespeicherten Dokumente pro Kunde schnell einige Megabyte anfallen. Die Antivirus-Lösung hat jedoch eine Größen-Obergrenze für Dateien, die in „Quarantäne“ aufgehoben oder hier hin verschoben werden. Die Folge: Die Antivirus-Lösung entschließt sich zur sofortigen, **unwiderruflichen Löschung** der „Datei, die von einer vermeintlich gefährlichen Datei verändert wurde“. In diesem Moment werden Ihre Kundendaten dauerhaft vernichtet, und das geschieht im Regelfall aufgrund der „bitte nicht nerven“-Einstellung der Antivirus-Lösung **ohne dass Sie überhaupt benachrichtigt werden**.

Es lässt sich leicht nachvollziehen, dass medo.check und unsere Support-Mitarbeiter gegen diesen Ablauf der Dinge machtlos sind, nachdem es einmal geschehen ist.

Aber: Sie können vorbeugen! Ihr Zeitaufwand: Einmalig 20 Minuten und 3 Minuten wöchentlich.

Was ist zu tun?

1. Machen Sie **regelmäßig Sicherungen** Ihrer Daten, völlig unabhängig davon, ob es sich um medo.check-Daten oder alle anderen Daten handelt. Sichern Sie diese Daten immer auf Datenträgern, die nicht dauernd angeschlossen an den PC oder das Stromnetz sind. (Denken Sie an Blitzschlag und Überspannung.) Am besten werden Sicherungs-Datenträger räumlich getrennt aufbewahrt, also in einer anderen Wohnung.
2. Überlegen Sie, welche Daten sie wie häufig sichern wollen. **Sichern Sie vor allem Daten und nicht Programme**. Programme erhalten Sie in der Regel immer wieder in der aktuellsten Version als Download – natürlich auch medo.check.

3. Stellen Sie für medo.check und andere branchenspezifische Anwendungen **Ausnahmen in Ihrer Antivirus-Lösung** ein.
4. Alle konkreten Vorgänge haben wir für Sie in **Anleitungen** hinterlegt:
<https://www.medocheck.com/wp-content/uploads/2022/02/medo.check-Backup.pdf>
<https://www.medocheck.com/wp-content/uploads/2021/07/Hinweise-zum-Umgang-mit-Antivirus-Loesungen.pdf>
5. Wenn Sie etwas nicht verstehen, holen Sie sich **Hilfe beim medo.check-Support**. Vereinbaren Sie einen Termin mit uns, sprechen Sie mit Ihrem IT-Verantwortlichen.

Verzichten Sie unter keinen Umständen auf eine fachgerechte Absicherung Ihrer Daten gegenüber Verlust, Diebstahl und Zerstörung.

Sie sollten sich gerade im Umgang mit Gesundheitsdaten auch Ihrer Sicherungspflicht aufgrund der DSGVO bewusst sein.

Lassen Sie sich das **Sicherungskonzept Ihres IT-Dienstleisters** erklären und stellen Sie es auf den Prüfstand bezüglich

- Datenverlust durch Blitzschlag, Brand, Diebstahl von Geräten, Diebstahl von Daten, Versagen von Geräten und Datenträgern.
- Datenverlust durch Verschlüsselung (Erpressung, sog. Verschlüsselungstrojaner.)
- Datenverlust durch eigenes Fehlverhalten aber auch Software-Fehler.

Konzepte zum Schutz und zur Sicherung der Ihnen anvertrauten Kundendaten sind **keine Sache von Verwandtschafts- oder Nachbarschaftshilfe**. Sie sollten sich fragen, ob der „Sohn ihres Bekannten“ bei Verlust haftet bzw. versichert ist.

Diese Aufgaben gehören unbedingt in professionelle Hände. Tatsächlich ist das Datensicherungskonzept Ihres IT-Betreuers nämlich Ihr Datensicherungskonzept.