

### Praxis Selbst-Check

Als Ihr Systemhaus sehen wir uns in der Pflicht, Sie vollumfänglich zu beraten und ggfls. Handlungsempfehlungen auszusprechen. Damit Sie einen ersten Überblick über die technische Situation in Ihrer Praxis haben, stellen wir Ihnen unseren Selbst-Check zur Verfügung.

#### Server

##### Wird der Server mit aktuellem Betriebssystem betrieben?

Server 2022	Server 2019	Server 2016	Server 2012

**Erklärung:** Veraltete Betriebssysteme werden nicht mehr supportet. Es gibt auch keine Sicherheitsupdates mehr. Aktuell ist Microsoft Server 2019 und 2022. Microsoft Server 2012 wird von Microsoft noch bis Januar 2023 eingeschränkt supportet und sollte spätestens bis dahin ausgetauscht worden sein.

##### Wie alt ist Ihr Server?

3 Jahre	5 Jahre

**Erklärung:** Um ein Ausfallrisiko zu minimieren, sollte ein Servertausch nach dem 3. Jahr überdacht werden.

##### Haben Sie eine tägliche Datensicherung mit Wechseldatenträgern?

Ja       Nein       Unbekannt

**Erklärung:** Bei Hardwaredefekten, Systemfehlern oder auch bei einem Hackerangriff hilft Ihnen eine Datensicherung vor möglichen wirtschaftlichen Schäden. Eine regelmäßige Überprüfung der Sicherung ist unerlässlich. Eine verschlüsselte Kopie sollte immer außerhalb der Praxis aufbewahrt werden.

##### Haben Sie eine Regelung zur Mitnahme von Wechseldatenträgern (Datensicherung)?

Ja       Nein       Unbekannt

**Erklärung:** Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.

##### Haben Sie eine unterbrechungsfreie Stromversorgung (USV) im Einsatz?

Ja       Nein       Unbekannt

**Erklärung:** Bei plötzlichem Stromausfall besteht die Gefahr von Datenverlust oder Programm-/Datenbankproblemen. Eine unterbrechungsfreie Stromversorgung stellt sicher, dass alle Programme geschlossen werden und der Server wird heruntergefahren.

## Jupitec GmbH

### Arbeitsplätze

Werden alle PCs mit aktuellen Windows-Betriebssystem betrieben?

Windows 10/Windows11	Windows 8.1	Windows 7
----------------------	-------------	-----------

**Erklärung:** Veraltete Betriebssysteme werden nicht mehr supportet. Es gibt auch keine Sicherheitsupdates mehr. Aktuell sind Windows 10 PRO und Windows 11 PRO für MEDICAL OFFICE freigegeben.

Wie alt sind Ihre Arbeitsplätze?

3 Jahre	5 Jahre
---------	---------

**Erklärung:** Um ein Ausfallrisiko zu minimieren, sollte ein Arbeitsplatz ca. alle 5 Jahre getauscht werden.

### IT-Sicherheit

Die aktuelle Bedrohungslage und die RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT der KBV stellen die IT-Sicherheit in einer Arztpraxis auf den Prüfstand. Hier erhalten Sie einen Überblick, ob Sie die Richtlinien einhalten und wie sicher Ihre IT ist.

#### Verschlüsselung der Daten

Steht Ihr Server in einem abschließbaren Serverschrank?

- Ja       Nein       Unbekannt

Ist Ihr Notebook mit Bitlocker und Zwei-Faktor-Authentisierung gesichert?

- Ja       Nein       Unbekannt

Ist Ihre Datensicherung verschlüsselt?

- Ja       Nein       Unbekannt

**Erklärung:** Die Verschlüsselung der Daten auf den Datenträgern schützt vor unberechtigten Zugriff.

### Virenschutz

Haben alle Server und alle Arbeitsplatzrechner eine aktuelle, aktive Virensignatur?

- Ja       Nein       Unbekannt

## Jupitec GmbH

### Überprüfen Sie regelmäßig die Aktualität?

Ja  Nein  Unbekannt

**Erklärung:** Da Computerviren ständig mutieren, können nur aktuelle AntiVirusProgramme auf die Bedrohung reagieren. Nur wenn alle Server und Arbeitsplätze in einem Netzwerk über einen aktiven, aktuellen Virenschutz verfügen, kann dies Sicherheit bieten. Ein Virus kann über das Netzwerk nicht geschützte Clients infizieren. Eine regelmäßige Prüfung ist unerlässlich.

### Hardwarefirewall

#### Schützt eine Hardwarefirewall den Übergang zum Internet?

Ja  Nein  Unbekannt

**Erklärung:** Zum Schutz der sensiblen Patientendaten ist eine Hardwarefirewall die Voraussetzung gemäß der Richtlinie § 75b SGB V. Der Übergang zu anderen Netzen insbesondere das Internet muss durch eine Firewall geschützt werden.

### Netzwerksicherheit

#### Haben Sie einen Netzwerkplan?

Ja  Nein  Unbekannt

**Erklärung:** Gemäß der Richtlinie § 75b SGB V. ist das interne Netz inklusive eines Netzplanes zu dokumentieren.

#### Setzen Sie ein umfassendes Monitoring ein?

Ja  Nein  Unbekannt

**Erklärung:** Durch die Verwendung von Monitoring-Software können Probleme frühzeitig erkannt und proaktiv beseitigt werden. Hierdurch kann verhindert werden, dass diese Ihre Arbeitsabläufe stören oder größeren Schaden anrichten.

#### Verwenden Sie eine Authentisierung?

Ja  Nein  Unbekannt

**Erklärung:** Gemäß der Richtlinie § 75b SGB V: für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden. Eine geeignete Authentisierung für Benutzerkonten sind Passwörter mit mehr als 12 Zeichen inklusive Sonderzeichen und Zahlen.

### Weitere Punkte

#### Halten Sie den Status Ihrer eingesetzten Software (z.B. Java) immer aktuell?

Ja  Nein  Unbekannt

**Erklärung:** Mit den Updates und Aktualisierungen werden oftmals Sicherheitslücken (Log4J) geschlossen.

**Gibt es unterschiedliche Windows-Benutzer für Desktop PC und Server? Hat der Benutzer „Praxis“ Administratorrechte auf dem Medical Office Server?**

Ja             Nein             Unbekannt

**Erklärung:** Um zu verhindern, dass sich Schadprogramme von den Anwendungs-PCs auf den Server ausbreiten können, sollte der Benutzer „Praxis“ keine administrativen Rechte auf dem Medical Office Server haben.

**Wird der Arbeitsplatz bei Nichtbenutzung gesperrt?**

Ja             Nein             Unbekannt

**Erklärung:** Um Patienten keinen Zugriff auf Ihren PC zu gewähren, sollten PCs, insbesondere unbeaufsichtigte, nach Benutzung gesperrt werden.

**Werden Handys/Tablets bei Nichtbenutzung gesperrt?**

Ja             Nein             Unbekannt

**Erklärung:** Um Patienten keinen Zugriff auf das Handy/Tablet zu gewähren, sollten diese, insbesondere unbeaufsichtigte, nach Benutzung gesperrt werden.

**Können unberechtigte Personen Einblick auf Monitore nehmen?**

Ja             Nein             Unbekannt

**Werden Passwörter im Browser gespeichert?**

Ja             Nein             Unbekannt

**Erklärung:** Daten die im Browser gespeichert werden, werden nicht lokal auf Ihrem PC sondern auch beim Hersteller/Betreiber des Browsers gespeichert.

**Werden Nutzerdaten automatisch online Synchronisiert?**

Ja             Nein             Unbekannt

**Erklärung:** Cloud-Dienste wie One-Note oder Dropbox sollten nicht genutzt werden, da Ihre Daten außerhalb Ihrer Reichweite auf den Server des Betreibers der Cloud gespeichert werden.