

Webinar #7/2022

Wir freuen uns, dass Sie heute dabei sind



Wir starten um 18:30 Uhr

Willkommen beim od – Webinar #07/2022

byzz® Workshop

- >> Datenaustausch aus und in die Praxis
- >> Optimierung des digitalen byzz® Workflows
- >> Daten-Backup: Das ewige Thema
- >> Toolbar anpassen (optional)

Ihre Moderatoren heute Abend



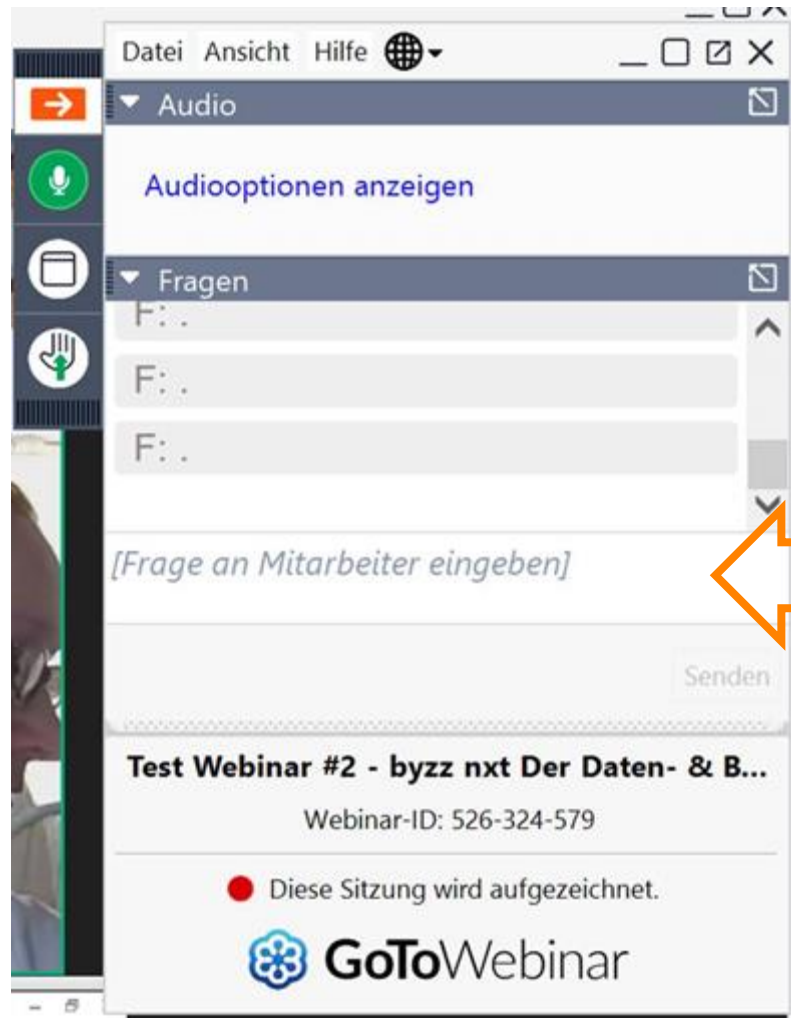
Jan Kliewer



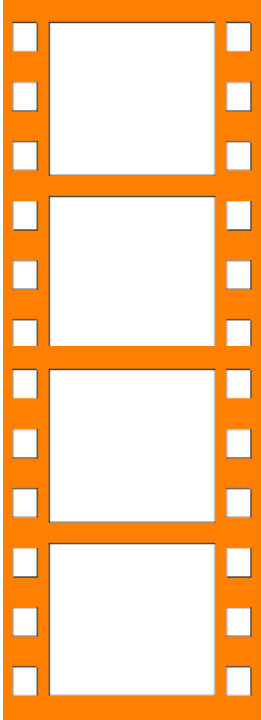
Andreas Möller



1. Bitte klicken Sie für Ihre Frage hier.



2. Stellen Sie uns die Ihre Fragen im Fragen-Fenster



Sie erhalten das komplette, heutige Webinar als Video-Aufzeichnung zum späteren Anschauen.

Natürlich können Sie dieses Video auf für Ihre internen Praxis-Schulungen benutzen.





Ihre Meinung ist uns sehr wichtig.

Bitte nehmen Sie an der Umfrage nach dem Webinar teil.

>> Und nun geht es los ...

>> Umfrage 1 - Datenaustausch aus und in die Praxis

1 von 2. Wie versenden Sie Ihre Daten an andere Praxen, Labore oder Patienten?

Multiple-Choice mit mehreren Antworten

66.67%

Mail (Outlook / Thunderbird) verschlüsselt

25%

WeTransfer o.ä.

50%

7-Zip mit Passwort

33.33%

CryptShare

8.33%

eigener FTP oder Cloud

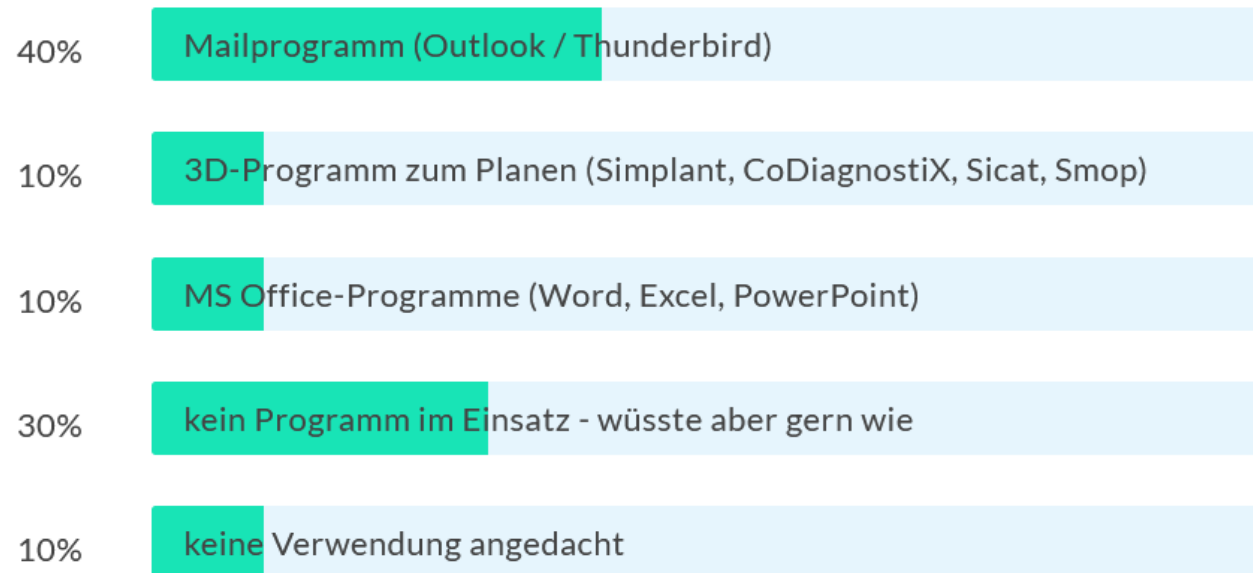
Live - Datenaustausch aus und in die Praxis

- >> Versenden und Empfangen von Daten
- >> Daten beim Senden verschlüsseln (Outlook / Thunderbird)
- >> CryptShare express (WebAccess)
- >> Mit TransCrypt Daten bis 2GB versenden

>> Umfrage 2 - Optimierung des digitalen byzz® Workflows

2 von 2. Welche Programme haben Sie im Einsatz, die Sie von byzz aus starten (inkl. Datenaustausch)?

Multiple-Choice mit einer Antwort



Live - Optimierung des digitalen byzz® Workflows

- >> Verwendung von Drag & Drop / Bildseitenleiste
- >> Externe Programme, inklusive Datenübergabe

Backup - Das ewige Thema ...

Kein Backup – kein Mitleid !!



Warum sollte ich meine Daten sichern – was kann mir schon passieren:

>> Elementare Schäden (Wasser / Feuer)

>> Einbruch / Diebstahl

>> Verschleiß (MTBF)

>> Viren, Trojaner, Ransomware

Wie kann ich meine Daten heutzutage sicher verwahren:

>> Bänder (bis 32 TB möglich)

>> Externe Festplatte(n)

>> NAS (Network Attached Storage)

>> In der Cloud

und mit welchem Zeitplan / Rhythmus

Welche Backup-Zeitplan / -Rhythmus ist sinnvoll?

>> täglich

>> wöchentlich

>> quartalsweise

>> jährlich

Die sinnigste Frage ist hier wahrscheinlich, wie kann ich den monetären Verlust, durch einen Praxisausfall, bei einem Datenverlust, maximal minimieren.

Was ist das wichtigste, wenn das Backup eingerichtet ist und funktioniert?

Was ist das wichtigste, wenn das Backup eingerichtet ist und funktioniert?

Die Datenkontrolle !!!

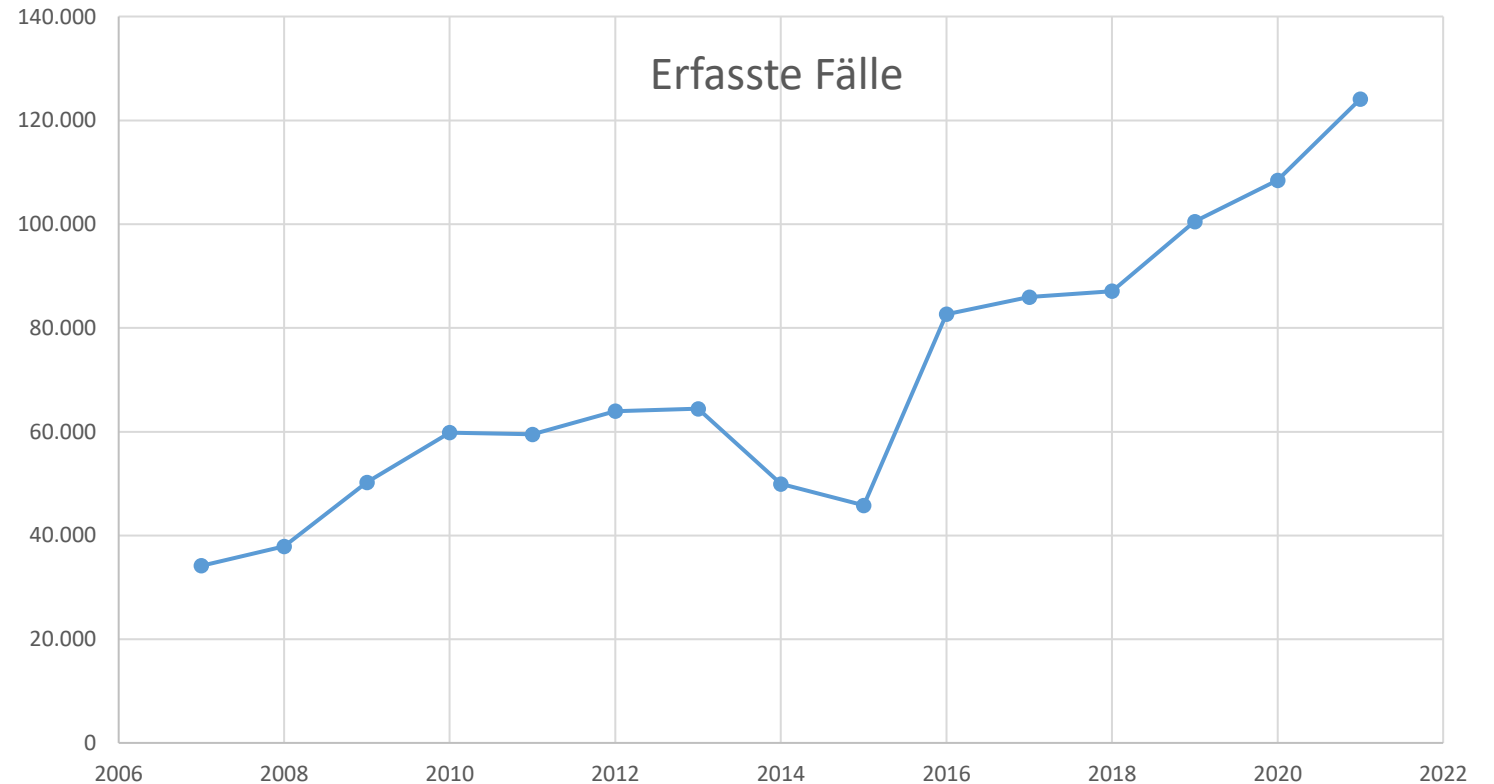
Was ist das wichtigste, wenn das Backup eingerichtet ist und funktioniert?

Was nützt die beste Hardware, wenn die Daten nicht oder unvollständig gesichert werden / wurden.

Die 1-Millionen-Dollar-Frage:

Wer schaut sich in Ihrer Praxis die Protokolle regelmäßig an?

Weitere Gründe, warum wir uns mit Datensicherung beschäftigen sollten:

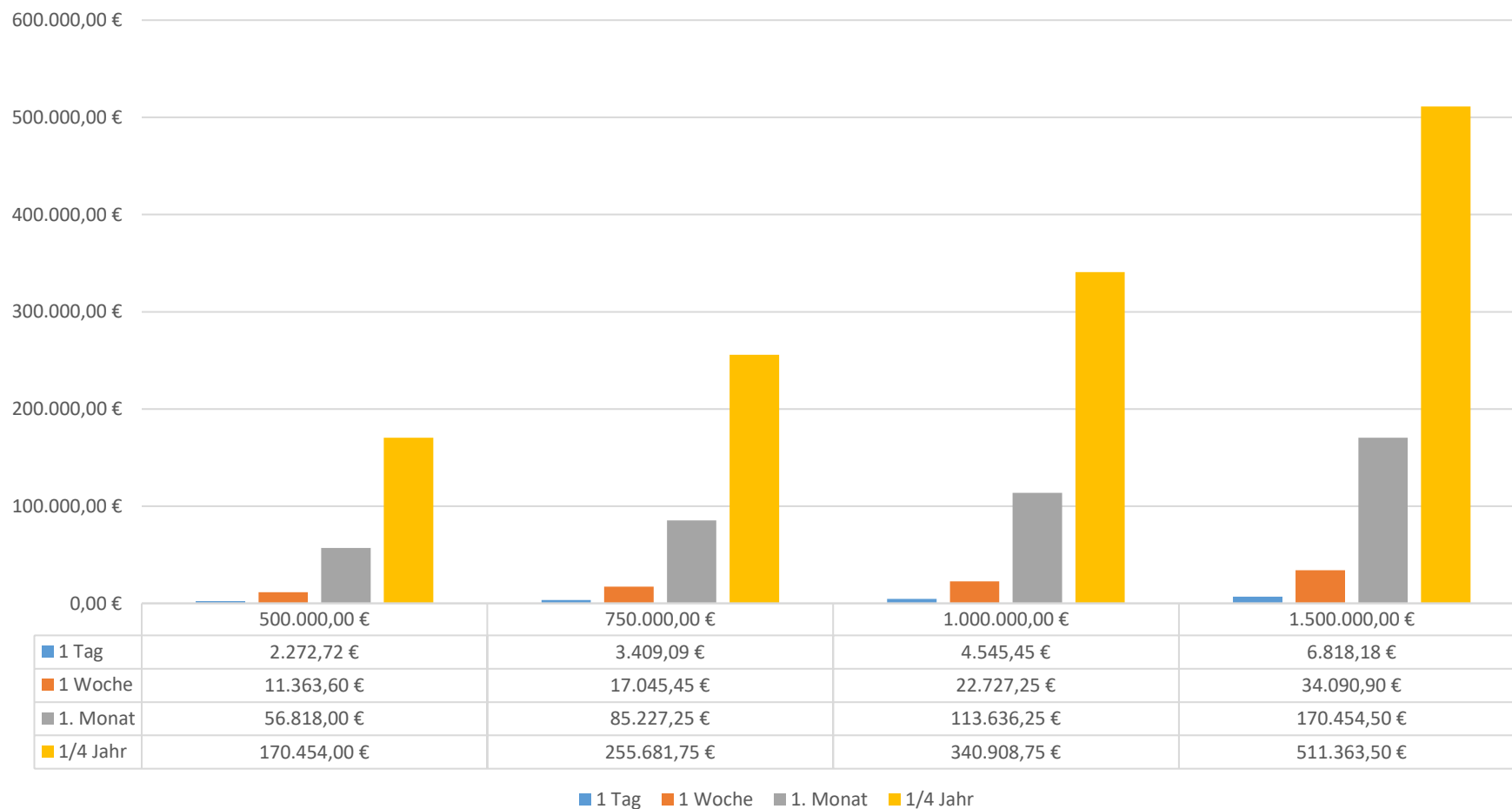


Die polizeilich erfasste Fälle von Cyberkriminalität im engeren Sinne in Deutschland von 2007 bis 2021

Weitere Gründe, warum wir uns mit Datensicherung beschäftigen sollten:

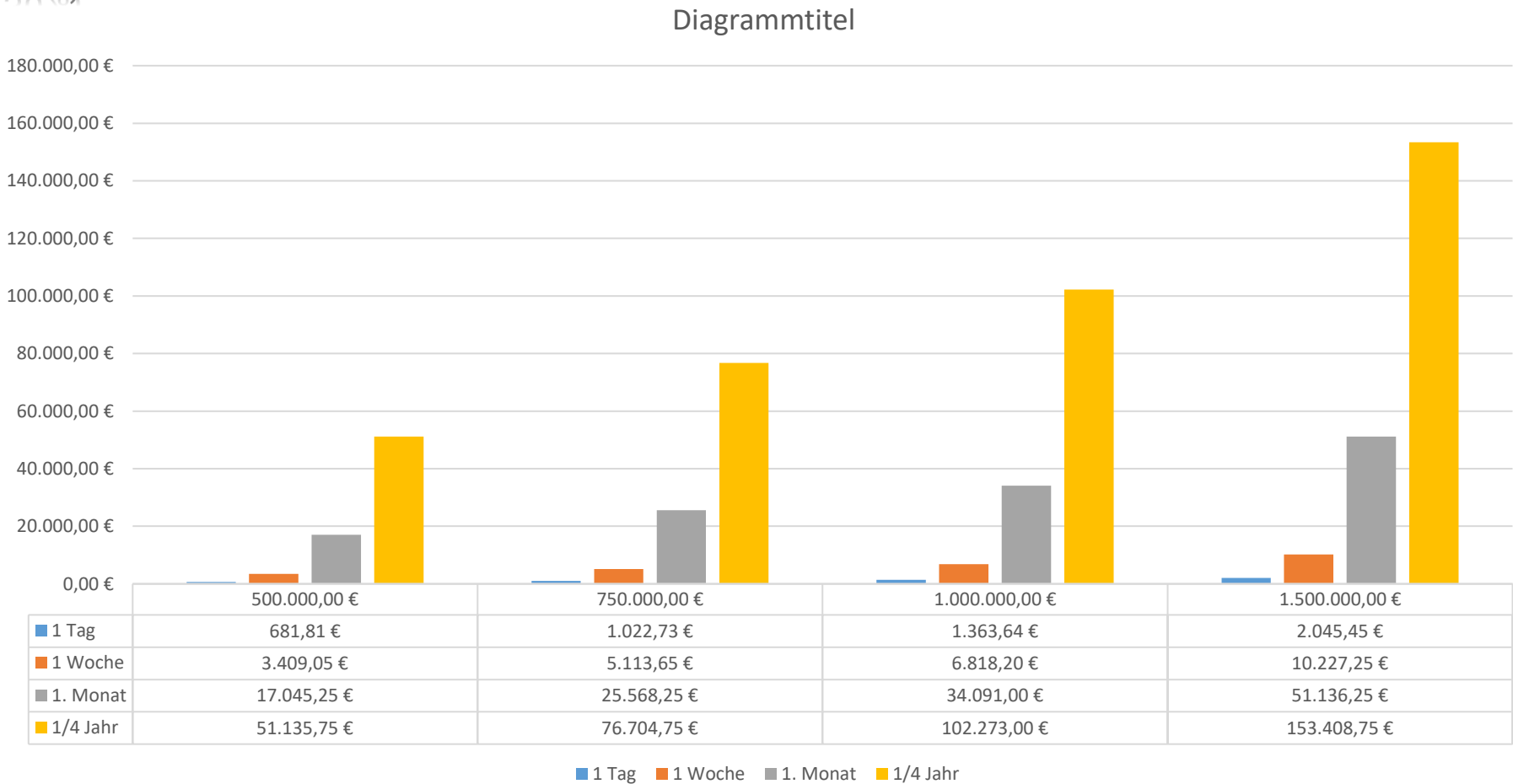
- >> Die Anzahl erfasster Cyberstraftaten steigt weiter an - im Jahr 2021 um über 12 %
- >> Cybercrime und -angriffe sind in Folge von COVID-19 um 600% gestiegen
- >> Experten schätzen, dass im Jahr 2022 alle 11 Sekunden ein Ransomware-Angriff stattfinden wird
- >> Die durchschnittliche Ausfallzeit nach einem Angriff beträgt 21 Tage
- >> Die Angriffe / Angriffsziele werden immer mehr automatisiert durch Sniffer- und Portscanner-Programme

Der wirtschaftliche Aspekt - Umsatzeinbußen:



Der wirtschaftliche Aspekt – Gewinnverlust:

(Deckungsbeitrag 30%)



Was können wir für Sie zu diesen Thema beisteuern?

byzz nxt ab Version 13x ...

Automatische Datensicherung jeden Mittag

Checkliste Datensicherheit

- ✓ Wird die AV-Software regelmäßig aktualisiert?
- ✓ Ist eine Firewall integriert und up to date (Firmware usw.)?
- ✓ Sind die Mitarbeiter zum Thema „Erkennen von Phishing-Mails“ geschult?
- ✓ Gibt es einen Notfallplan bei Datenüberfällen?
- ✓ Werden die Daten regelmäßig gesichert und geprüft?
- ✓ Werden alle Updates (PVS, BVS, OS) regelmäßig aktualisiert?
- ✓ Werden die, in der Praxis verwendeten Passwörter, regelmäßig gewechselt (Passwort-Tresor)?
- ✓ Sind die Praxis-Rechner vor unberechtigten Zugriffen geschützt (Screensaver, USB-Anschluss gesperrt)?
- ✓ Gibt es einen Datenschutz- / Cyberschutzbeauftragten?
- ✓ Wurden die Richtlinien gemäß der IT-Sicherheitsrichtlinien (§75b SDG V) umgesetzt?
- ✓ Liegt die Konformitätsbescheinigung gemäß der jährlichen Evaluationspflicht (§75b SDG V) vor?

>> Frage aus dem letzten Webinar:

Wie kann ich die Toolbar ändern?

Melden Sie sich an:

Webinar #8/2022: byzz Workshop Röntgen / Konstanzprüfung

<https://attendee.gotowebinar.com/register/2636879997652815375>

Nach der Anmeldung erhalten Sie eine Bestätigung per E-Mail mit Informationen zur Teilnahme.

Wir freuen uns über Ihre Meinung und Kritik.

Ihr Feedback können Sie selbstverständlich vollkommen anonym abgeben

Wohltuende Kritik ist
konstruktiver als jedes Lob.

od-Webinar



Danke für Ihre Aufmerksamkeit.

Wir wünschen Ihnen einen schönen Feierabend und bleiben Sie und Ihr Team weiterhin gesund.

Ihr orangedental Team

Sie finden unsere News auch über:

