# Digitale Zahnlücke: Wie sicher ist Ihre Praxis-IT?

## Die neue IT-Sicherheitsrichtlinie - Live-Hacking & Einfache Lösungen

Richard Marnau

19.11.2025

# Agenda

Warum? Wieso? Weshalb? Was gilt für mich?

Struktur & Rechtsrahmen Praxisgrößen, Aufbau der Anlagen

Anlage 1, 2 und 3 –Anforderungen nach Praxisgröße

Praxisbeispiele – Live Hacking & Phising

Zusammenfassung und Fahrplan -> Was ist konkret zu tun?

Frage und Antworten

# Art. 32 DSGVO Sicherheit der Verarbeitung

(1) Unter **Berücksichtigung des Stands der Technik**, der **Implementierungskosten** und der **Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung**

sowie der **unterschiedlichen Eintrittswahrscheinlichkeit** und **Schwere des Risikos** für die **Rechte und Freiheiten natürlicher Personen**

treffen **der Verantwortliche** und der Auftragsverarbeiter geeignete **technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;

DSGVO / BDSG erfordern, dass die Praxis technische und organisatorische Maßnahmen zur Sicherheit der IT durchführt. (**Art. 32 DSGVO) – Doch was genau ist damit gemeint?**

**Die IT-Sicherheitsrichtlinie setzt hier einen Standard und konkretisiert diese.**

Rechtsgrundlage: § 390 SGB V

Veröffentlicht: 1.7.2025

geänderte Anforderungen: verbindlich ab 2.1.2026

Schutzziele: Vertraulichkeit Integrität, Verfügbarkeit

# Definition der Praxisgrößen:

Es zählen die Mitarbeiter, die “ständig mit der Datenverarbeitung betraut sind”.

Gleiche Zählung wie z.B. bei der DSGVO / Datenschutzbeauftragten

Alle ZFA’s und Behandler, Auszbuildenden, Abrechnungshelfer etc.

Nicht: Reinigungsfachkraft, Hausmeister etc..

# Aufbau der Richtlinie

Maßnahme A1, A2 und A3 gelten für folgende Praxisgrößen

A1- Praxis “Klein” bis 5

A2 - Praxis “Mittel” 6–20

A3 - Praxis “Groß” >20

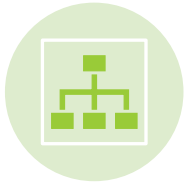
Anlage 4 (Großgeräte) - CT, MRT, PET, LINAC

Anlage 5 (alle da TI)

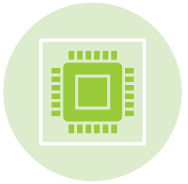
# Agenda

Anlage 1 Kernanforderungen

# Anlage 1: Überblick



Personal & Organisation
(A1-01/10)



Netz & Updates (A11-17)

Endgeräte & Sicherung (A1-18/25)

Zugriffe, Mobile & Versand
(A1-26/39)

E-Mail & Cloud (A1-40/50)

# Anlage1 – Alle Praxen

## (A1-01) Geregelte Einarbeitung neuer Mitarbeitender (neu)

- Mitarbeitende werden zu Beginn ihrer Tätigkeit in ihre Aufgaben sowie die geltenden Regelungen und Verfahren eingewiesen.
- Empfehlung: Private Nutzung der Computer schriftlich verbieten!

## (A1-02) Verfahren beim Weggang von Mitarbeitenden (neu)

- Ausscheidende Mitarbeitende müssen alle erhaltenen Unterlagen zurückgeben. Genutzte Zugangsdaten sind zu ändern oder zu löschen.
- Empfehlung: Checkliste, VPN und Laptops nicht vergessen (!)

# Anlage1 – Alle Praxen

**A1-03 Festlegung von Regelungen zum Einsatz von Fremdpersonal (neu)**

- Externes Personal muss dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten.

**A1-04 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal (neu)**

- Bevor externe Personen Zugang und Zugriff zu vertraulichen Informationen erhalten, müssen mit ihnen Vertraulichkeitsvereinbarungen in schriftlicher Form geschlossen werden.
  - Muster unter: https://compfair.de/muster.zip

# Anlage1 – Alle Praxen

## A1-05 Verpflichtung und Zuständigkeiten von Mitarbeitenden (neu)

- Alle Mitarbeitenden müssen dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Die Aufgaben von Mitarbeitenden müssen dokumentiert sein.
  - Muster: https://compfair.de/muster.zip

## A1-06 Qualifikation des Personals (neu)

- Mitarbeitende müssen regelmäßig geschult bzw. weitergebildet werden, insbesondere auch in Bezug auf die eingesetzte Technik/IT.
  - Online Kurse sind zulässig

# Anlage1 – Alle Praxen

**A1-07 Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden (neu)**

- Bei der Einstellung neuer Mitarbeitenden sollte besonders auf ihre Vertrauenswürdigkeit, beispielsweise bei der Prüfung vorliegender Arbeitszeugnisse, geachtet werden.

**A1-08 Sensibilisierung der Praxisleitung für Informationssicherheit (neu)**

- Die Praxisleitung muss ausreichend für Sicherheitsfragen sensibilisiert werden. Sicherheitskampagnen oder andere Schulungsmaßnahmen müssen von der Praxisleitung unterstützt werden.

**A1-09 Einweisung des Personals in den sicheren Umgang mit TI (neu)**

- Alle Mitarbeitenden und externen Benutzenden müssen in den sicheren Umgang mit IT-Komponenten eingewiesen und sensibilisiert werden, soweit dies für ihre Arbeitszusammenhänge relevant ist.

# Anlage1 – Alle Praxen

**A1-10 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit (neu)**

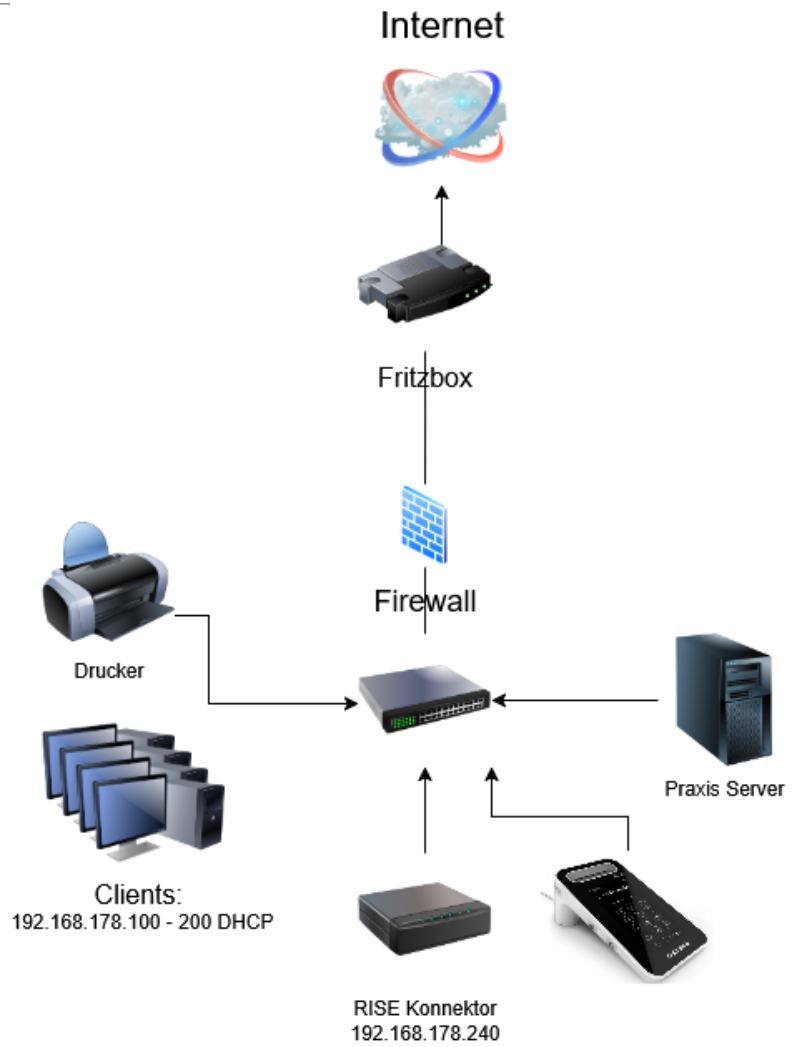
- Alle Mitarbeitenden sollten geschult werden.

**A1-11: Absicherung der Netzübergangspunkte**

- Firewall sollte vorhanden sein

**A1-12: Dokumentation des Netzes**

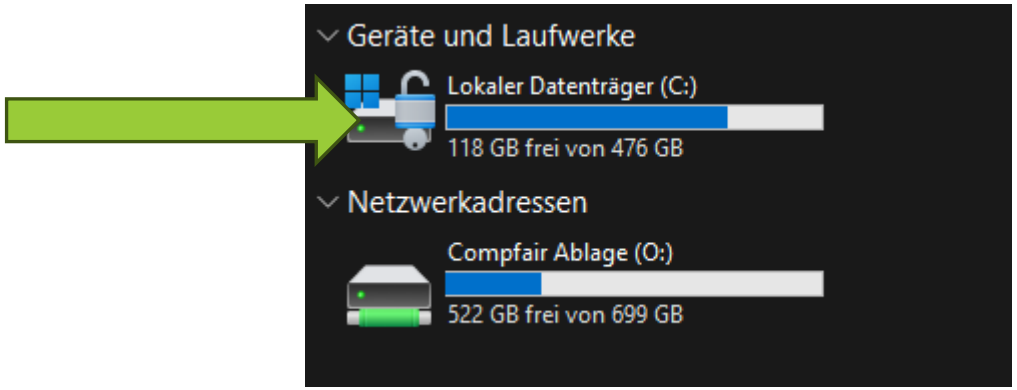
- Netzwerkplan z.B. via https://draw.io + IP Adressplan



# Anlage1 – Alle Praxen

**A1-13 Grundlegende Authentisierung**

- Login Password bei Windows.
  Nicht „praxis“. Besser „Praxis0111#“
- KEIN Windows Password ist sicher
- Verschlüsselung erforderlich (Bitlocker)
- Test: Windows Taste + E -> „Dieser PC“



# Anlage1 – Alle Praxen

**A1-14 Installation von Updates (neu)**

- Automatische Updates aktivieren oder IT-Unternehmen beauftragen (Wartung)

**A1-15 Verantwortlichkeit für Updates (neu)**

- Es muss festgelegt werden, wer die Updates installiert.

**A1-16 Identifizierung ausbleibender Updates (neu)**

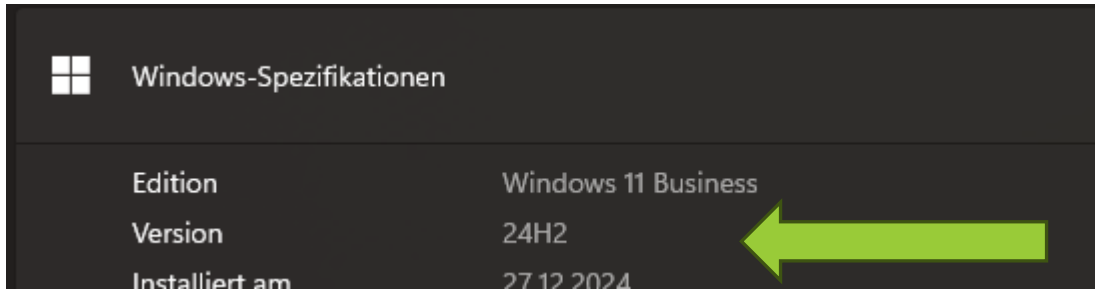
- EDV, die keine Sicherheitsupdates mehr erhält muss identifiziert werden.
  - **Aktuelles Beispiel**: Windows 10, Office 2016, Office 2019

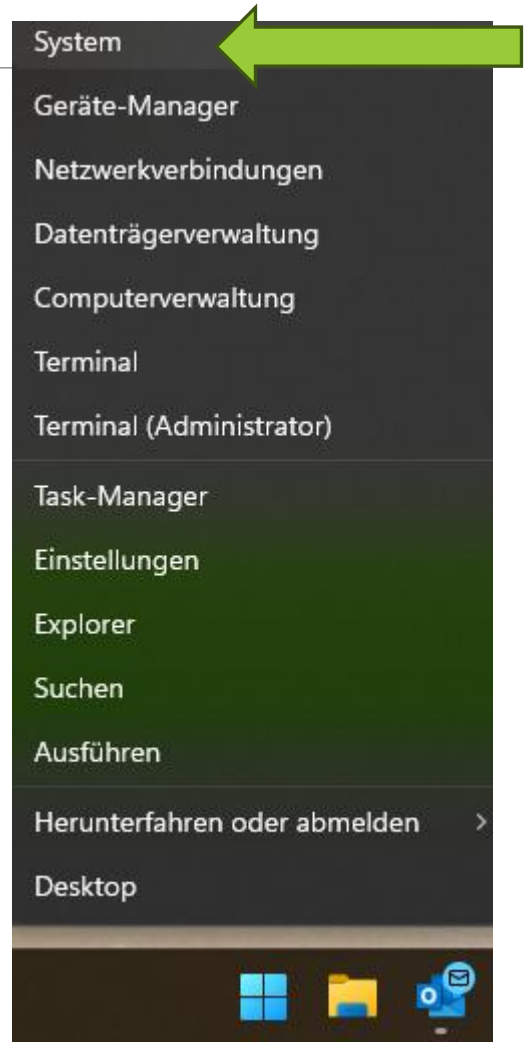
**A1-17 Ausmusterung oder Separierung bei ausbleibenden Updates (neu)**

- Systeme, die keine Sicherheitsupdates mehr erhalten, müssen ausgemustert **oder** separiert in einem eigenen Netzwerksegment betrieben werden.

# Aktuell Windows 10

- **Windows 10** erhält keine Sicherheitsupdates mehr – 14. Oktober 2025
- **Windows 11 23H2** erhält keine Sicherheitsupdates mehr – 11.11.2025
  - Test mit Windowstaste + X, und System auswählen



# Netz & Updates

- **A1-18: Verhinderung der unautorisierten Nutzung von Mikrofonen und Kameras**
  - Standardeinstellung in Windows, Anwendung müssen ein Zugriff erfragen:
  - Tipp: Windowstaste (Startmenü) -> Mikrofone eingeben. Einstellung prüfen.
- **A1-19: Abmelden nach Aufgabenerfüllung**
  - Abmeldung unter Windows wegen langer Startzeit problematisch. Praxisprogramm prüfen, automatische Sperre des Computers einrichten.
- **A1-20: Einsatz von Virenschutzprogrammen**
  - **Mehr dazu in Praxis Beispiel2**

# Datensicherung – Die Lebensversicherung

## A1-21 Regelmäßige Datensicherung

- Sämtliche relevante Daten sind regelmäßig zu sichern.

## A1-22 Schutz der Datensicherung **(neu)**

- Die Datensicherung muss vor unbefugtem Zugriff gesichert werden.
  - Verschlüsselung der Datensicherung zwingend erforderlich!

## A1-23 Art der Datensicherung **(neu)**

- Es muss festgelegt werden, wie die Daten abgesichert werden

## A1-24 Verantwortliche der Datensicherung **(neu)**

- Es muss festgelegt werden, wer für die Datensicherung zuständig ist.

## A1-25 Test der Datensicherung **(neu)**

- Es sollte getestet werden, ob Daten wiederherstellbar & vollständig vorhanden sind.
  - Test-Wiederholungen durchführen: Alle 6 Monate vollständiger Test der Wiederherstellbarkeit.
  - Tipp: Röntgen, QM, Abrechnung, Labor, Konstruktion, CadCam nicht vergessen. Liegt ggf. nicht auf dem Server

# Endgeräte & Sicherung

- **A1-26: Der Zugriff** auf Geräte und Software muss abgesichert werden
  - Nutzung von Berechtigungen in der Praxissoftware
- A1-27: **Konfiguration** von Synchronisationsmechanismen
  - Cloud Nutzung sollte vollständig deaktiviert werden. OneDrive deinstallieren
- A1-28: **Datei-** und Freigabeberechtigungen
  - Berechtigungen und Zugriffe vergeben. Beispiel: Praxisleitung und normaler Betrieb
- A1-29: **Datensparsamkeit**
  - So wenige personenbezogene Daten wie möglich sind zu verwenden.

# Mobilgeräte und Tablets

- **A1-30: Verwendung der SIM-Karten-PIN**
- A1-31: Sichere Grundkonfiguration für mobile Geräte
- **A1-32: Verwendung eines Gerätesperrcode**
- A1-33: Datenschutz-Einstellungen
- **A1-34: Sperrmaßnahmen bei Verlust**
  - Frei Haus verfügbar über Apple / Android
- A1-35: Sicherheit von Mobiltelefonen
- A1-42: Sichere Apps nutzen
- A1-43: Sichere Speicherung lokaler App
- A1-44: Verhinderung von Datenabfluss

# Wechseldatenträger / Speichermedien

- **A1-36: Schutz vor Schadsoftware**
  - Wechseldatenträger vor Nutzung überprüfen
- **A1-37: Angemessene Kennzeichnung der Datenträger beim Versand**
  - Keine personenbezogenen Daten auf Datenträger: „Befund Patient Müller Meier“
- **A1-38: Sichere Versandart und Verpackung**
  - Bitte versenden Sie keine Datensicherung per „Großbrief“ …
- **A1-39: Sicheres Löschen der Datenträger vor und nach der Verwendung**
  - USB Sticks in der Praxis sollten verschlüsselt sein (Bitlocker)
  - Alte Computer korrekt löschen vor Entsorgung (sofern nicht verschlüsselt)

# Internet-Anwendungen:

**A1-40 E-Mail-Client und –Server (später mehr) (neu)**

A1-41 Umgang mit Spam durch den Benutzenden **(neu)**

A1-44 Verhinderung von Datenabfluss

A1-45: Authentisierung bei Webanwendungen

A1-46: Schutz vertraulicher Daten

- *Sollten Sie als Praxis einen Webdienst anbieten..*

A1-47: Einsatz von Web Application Firewalls

A1-48: Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen

A1-49: Kryptografische Sicherung vertraulicher Daten

A1-50: Sicherheit von Cloud-Dienstleistern **(neu)**

- C5- Testat entsprechend §393 SGB V in Verbindung mit §384 SGB V

Agenda

# Anlage 2 und 3 zusätzliche Anforderungen nach Praxisgröße

# Anlage 2: Zusätzliche Anforderungen für mittlere Praxen

- **A2-01 Alarmierung und Logging**
  - Datensicherung mit täglicher E-Mail über Erfolg / Fehler
- A2-02 Nutzung von verschlüsselten Kommunikationsverbindungen
- **A2-03 Restriktive Rechtevergabe**
  - Arbeiten als lokaler Benutzer -> nicht mit Admin Rechten
- A2-04 Sichere zentrale Authentisierung in Windows-Netzen
- A2-05 **Richtlinie** für Mitarbeitende zur Benutzung von mobilen Geräten
- A2-06 Verwendung von Sprachassistenten
- A2-07 **Sicherheitsrichtlinien** und Regelungen für die Mobiltelefon-Nutzung
- A2-08 Sichere Datenübertragung über Mobiltelefone
- **A2-09 Regelung zur Mitnahmen von Wechseldatenträgern**
- A2-10 Minimierung und Kontrolle von App-Berechtigungen

# Anlage 3: Zusätzliche Anforderungen für Großpraxen

- A3-01 Messung und Auswertung des Lernerfolgs **(neu)**
- A3-02 Planung des Internen Netzwerkes **(neu)**
- A3-03 Absicherung von schützenswerten Informationen
- A3-12 Festlegung erlaubter Informationen auf mobilen Endgeräten **(neu)**
- **A3-13 Datenträgerverschlüsselung**
  - Wechseldatenträger sollten vollständig verschlüsselt werden.
- A3-14 Integritätsschutz durch Checksummen oder digitale Signaturen
- A3-15 Sicherer Betrieb von E-Mail Servern
- A3-16 Datensicherung und Archivierung von E-Mails
- **A3-17 Spam und Virenschutz auf dem E-Mail-Server**

# Anlage 3: Zusätzliche Anforderungen für Großpraxen

**Mobile Geräte:**

- A3-04 Festlegung einer **Richtlinie** für den Einsatz von Smartphones
- A3-05 Auswahl und Freigabe von Apps
- A3-06 Definition der erlaubten Informationen und Applikationen
- A3-07 Sichere Anbindung der mobilen Endgeräte an die Institution **(neu)**
- A3-08 Berechtigungsmanagement im MDM **(neu)**
- A3-09 Verwaltung von Zertifikaten
- **A3-10 Fernlöschung und Außerbetriebnahme von Endgeräten (neu)**
- A3-11 Auswahl und Freigabe von Apps (MDM)

# Anlage 3: Zusätzliche Anforderungen für Großpraxen

**A3-16 Datensicherung und Archivierung von E-Mails**

- Die Daten der E-Mail-Server und -Clients sind regelmäßig und verschlüsselt zu sichern.

**A3-17 Spam- und Virenschutz auf dem E-Mail-Server**

- Eingehende und ausgehende E-Mails und deren Anhänge sind auf Spam-Merkmale und schädliche Inhalte zu überprüfen. Diese Prüfung sollte zum Schutz des Clients auf dem Mail-Server erfolgen.

# Anlage 5: Dezentrale Komponenten der Telematikinfrastruktur (TI)

- A5-01 Planung und Durchführung der Installation
- A5-02 Betrieb (Dokumentation beachten)
- A5-03 Schutz vor unberechtigtem physischem Zugriff
- A5-04 Internet Verbindung parallel zur TI-Anbindung
- A5-05 Verbindung absichern (VPN-Tunnel zum TI-Gateway)
- A5-06 Beachtung der Vorgaben des TI-Gateway-Anbieters
- A5-07 Geschützte Kommunikation mit dem Konnektor
- **A5-08 Zeitnahes Installieren verfügbarer Aktualisierungen (Konnektor, Kartenleser)**
- **A5-09 Sicheres Aufbewahren von Administrationsdaten der TI**

Aus der Praxis

# Datenschutz, Virenschutz, IT-Berechtigungen, E-Mail/Phishing

# Praxis 1: Datensicherung

**Die Praxis Dr. Zahnstein wechselt einmal am Tag eine Festplatte am Server aus und erstellt damit eine Datensicherung.**

- Können die Daten wirklich wiederhergestellt werden? Ist die Festplatte möglicherweise leer oder die Daten unvollständig?
- Sind die Daten verschlüsselt, oder kann mit einer Festplatte die gesamte Praxis „gestohlen“ werden?
- Wer ist eigentlich für das wechseln verantwortlich?
- Was ist zu tun, um die Daten wiederherzustellen?
- *Maßnahmen:*
  - *A1-21-23: / Datensicherung  A3-13: / Verschlüsselung*
  - *A1-05: / Zuständigkeit*

# Praxis 1: Datensicherung

**„30-2-1 mit Schloss“-Regel als Minimum**

- Sie können **mindestens 30 Tage** rückwirkend Daten wiederherstellen
- Sie haben die Sicherung auf **2 verschiedenen Medien**
- **1 Sicherung ist extern** -> Gegen Brand/Wasserschaden/Diebstahl
- Alle Datensicherungen sind **verschlüsselt (Schlüssel ist dokumentiert)**
- **Datensicherungen müssen regelmäßig geprüft werden**
- **Achtung, z.B. die Dampsoft Sicherung ist nicht komplett**
  - Um die interne Datensicherung auf einem kleinen Datenträger realisieren zu können, werden vorhandene Bilder, Dokumente und alles auf dem Server nicht mitgesichert.

# Praxis 2: Virenschutz

**Praxis Dr. Zahnstein nutzt den internen Virenscanner: Microsoft Defender und fühlt sich gut geschützt.**

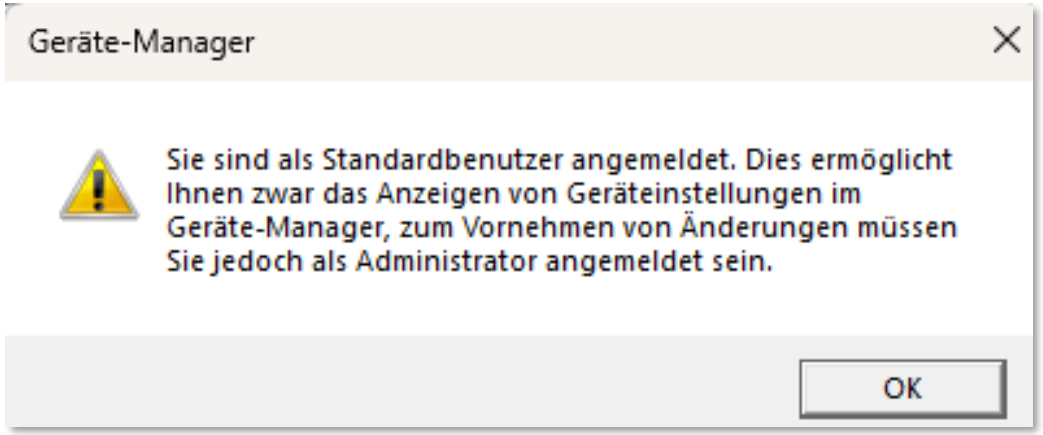
- Stimmt der Microsoft Defender schneidet bei Tests gut ab, ABER:
- Wer wird benachrichtigt, wenn ein Virus gefunden wird?
- Wer übernimmt die Konfiguration?
- **Zentrale Steuerung** und **Ereignisbenachrichtung** sind essenziel
- **Virenscanner auf dem Mailserver wichtig**
  - Ihr Hoster (1und1 / Strato / IONOS) hat das als kostenpflichtes Addon. **Essenziel**!
- *Maßnahmen: **A3-17 /** A1-20/40: Einsatz von **Virenschutzprogrammen***

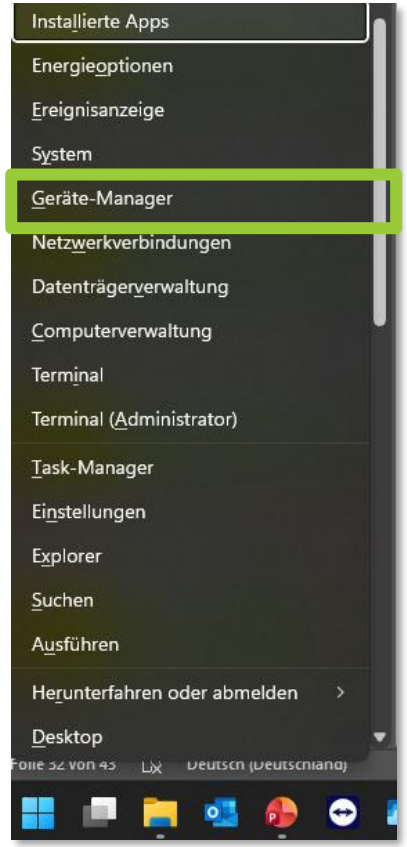
# Praxis 3: IT-Berechtigung

Alle Computer bei Dr. Zahnstein arbeiten mit beschränkten Berechtigungen. Haben Sie die auch ?

**Windows Taste + X** Drücken und **Geräte-Manager** auswählen.

- **A2-03 Restriktive Rechtevergabe**
- **A2-04 Sichere zentrale Authentisierung in Windows Netzen**



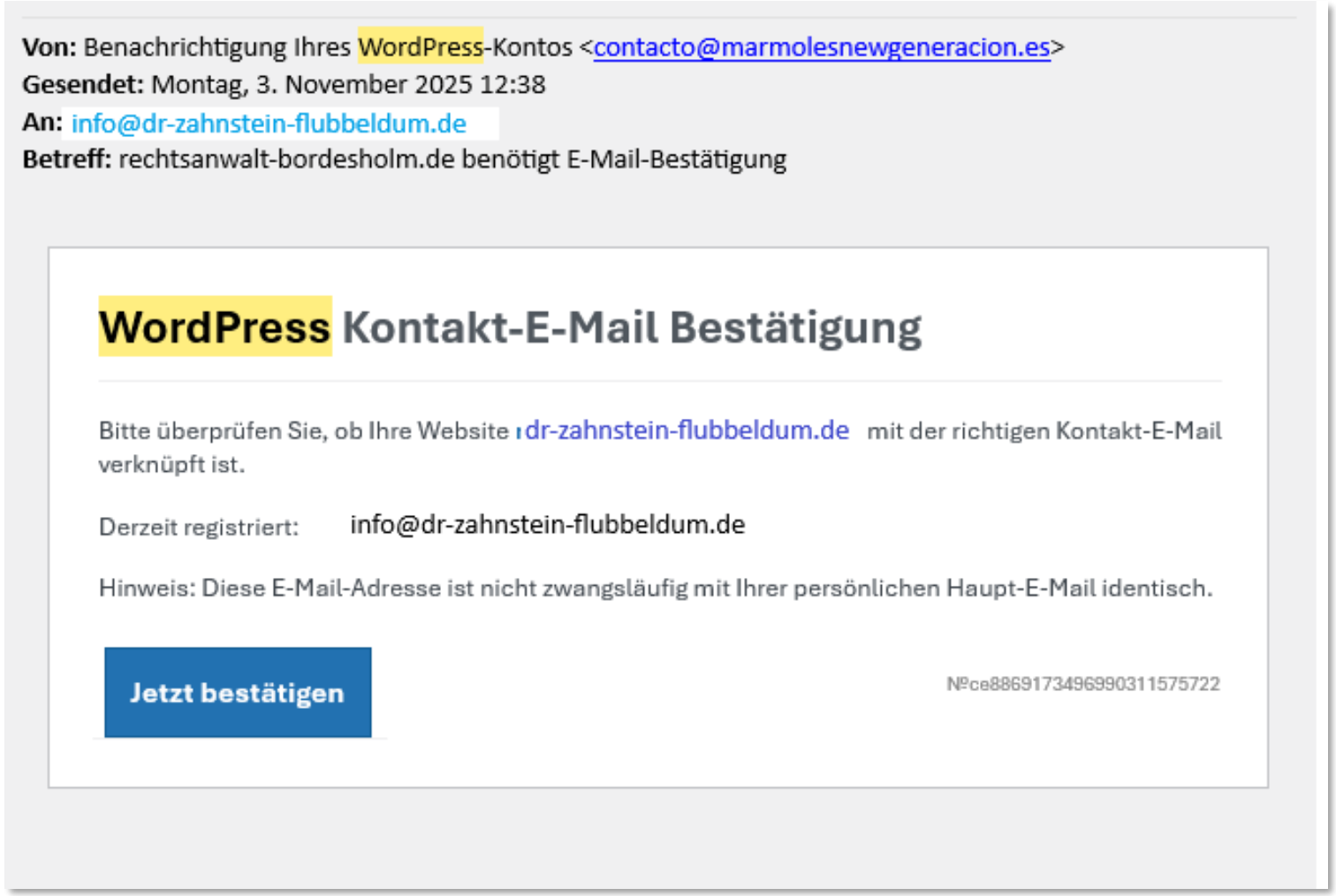
# Praxis 4: E-Mail / Phising

Die Zahnarztpraxis erhält eine E-Mail von Patienten, der um einen Termin bittet. Die E-Mail enthält im Anhang eine Word-Datei mit der Bezeichnung „Behandlungsdaten“.

**Maßnahmen**:

- *(A1-40) Sichere Konfiguration der E-Mail-Clients*
- *(A1-41) Umgang mit Spam durch Benutzende*
- *(A1-20) Einsatz von Virenschutzprogrammen*
- A1-(14-17) **Updates**
- **A1-17 Ausmusterung oder Separierung bei ausbleibenden Updates**
  - Office2016 und Office2019 ohne Sicherheitsupdates
  - **LibreOffice** oder **Thunderbird** als kostenlose Alternative

# Beispiele: E-Mail / Phising



**Von:** Benachrichtigung Ihres WordPress-Kontos <contacto@marmolesnewgeneracion.es>
**Gesendet:** Montag, 3. November 2025 12:38
**An:** info@dr-zahnstein-flubbeldum.de
**Betreff:** rechtsanwalt-bordesholm.de benötigt E-Mail-Bestätigung

**WordPress Kontakt-E-Mail Bestätigung**

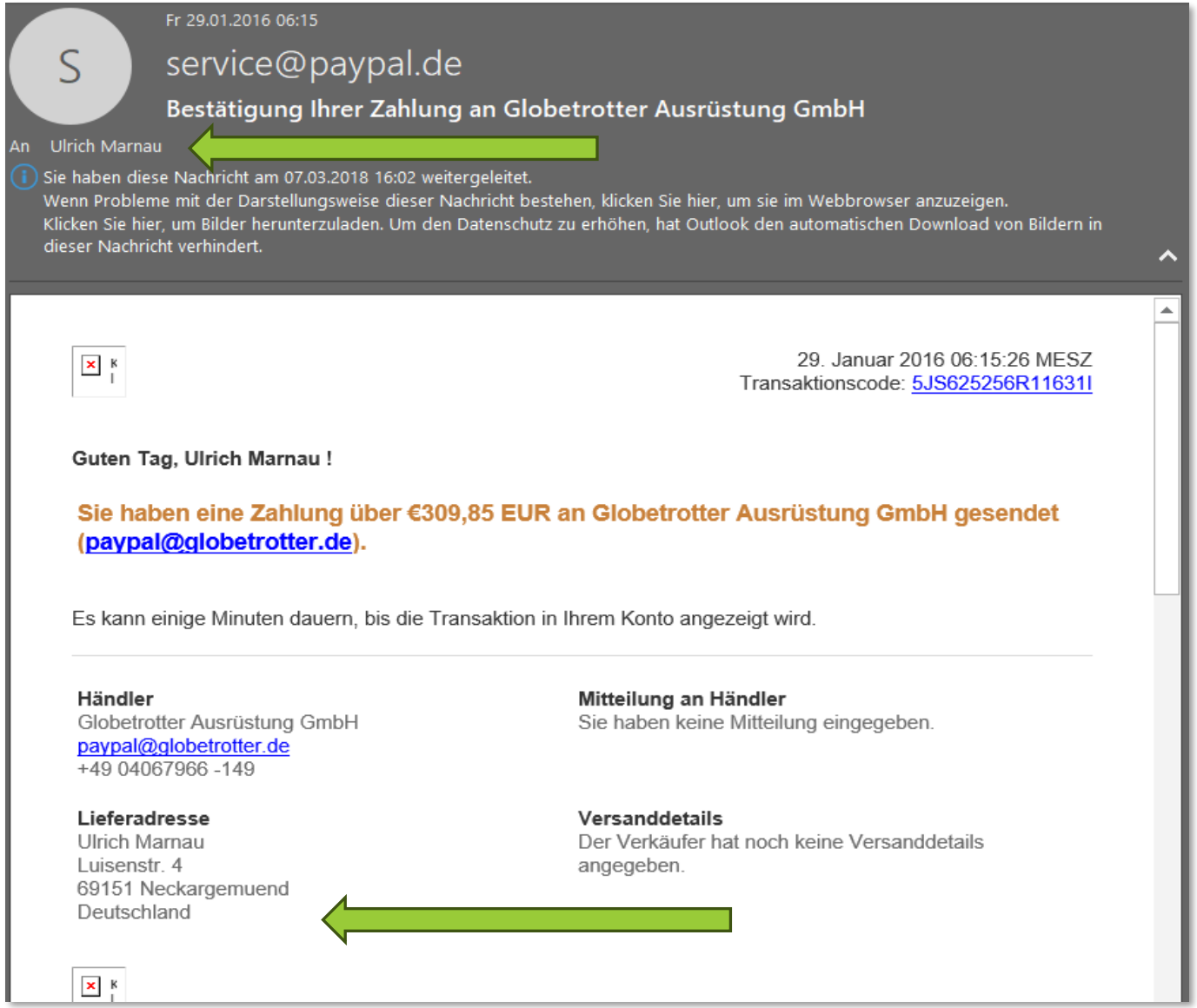
Bitte überprüfen Sie, ob Ihre Website dr-zahnstein-flubbeldum.de mit der richtigen Kontakt-E-Mail verknüpft ist.

Derzeit registriert: info@dr-zahnstein-flubbeldum.de

Hinweis: Diese E-Mail-Adresse ist nicht zwangsläufig mit Ihrer persönlichen Haupt-E-Mail identisch.

**Jetzt bestätigen**

№ce886917349699031157572 2



Fr 29.01.2016 06:15

S

service@paypal.de

**Bestätigung Ihrer Zahlung an Globetrotter Ausrüstung GmbH**

An Ulrich Marnau

Sie haben diese Nachricht am 07.03.2018 16:02 weitergeleitet.
Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

29. Januar 2016 06:15:26 MESZ
Transaktionscode: 5JS625256R11631I

**Guten Tag, Ulrich Marnau !**

**Sie haben eine Zahlung über €309,85 EUR an Globetrotter Ausrüstung GmbH gesendet (paypal@globetrotter.de).**

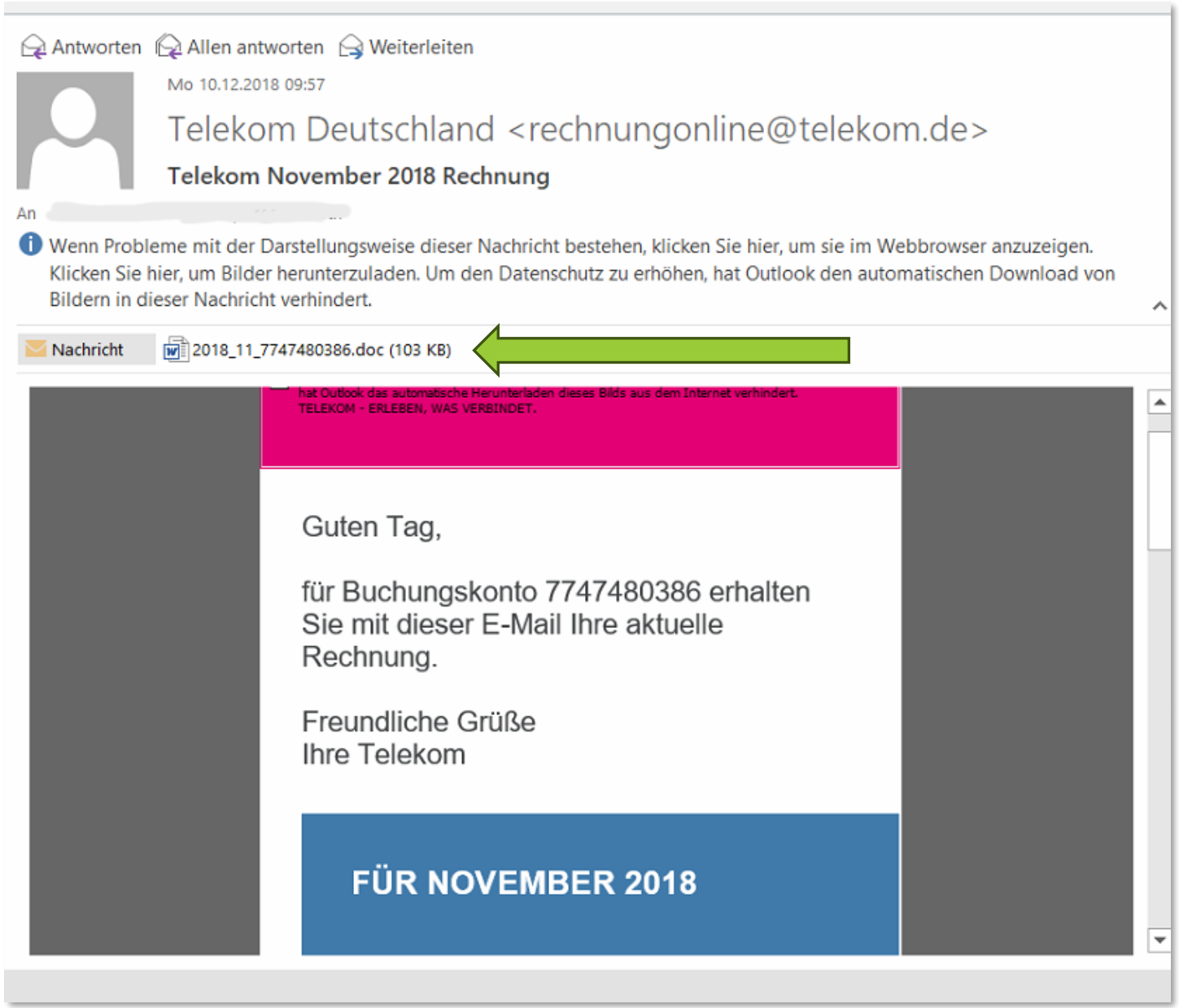
Es kann einige Minuten dauern, bis die Transaktion in Ihrem Konto angezeigt wird.

**Händler**
Globetrotter Ausrüstung GmbH
paypal@globetrotter.de
+49 04067966 -149

**Mitteilung an Händler**
Sie haben keine Mitteilung eingegeben.

**Lieferadresse**
Ulrich Marnau
Luisenstr. 4
69151 Neckargemuend
Deutschland

**Versanddetails**
Der Verkäufer hat noch keine Versanddetails angegeben.


Antworten
Allen antworten
Weiterleiten
Mo 10.12.2018 09:57
Telekom Deutschland <rechnungonline@telekom.de>
Telekom November 2018 Rechnung
An
Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen. Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.
Nachricht
2018_11_7747480386.doc (103 KB)
hat Outlook das automatische Herunterladen dieses Bilds aus dem Internet verhindert.
TELEKOM - ERLEBEN, WAS VERBINDET.
Guten Tag,
für Buchungskonto 7747480386 erhalten Sie mit dieser E-Mail Ihre aktuelle Rechnung.
Freundliche Grüße
Ihre Telekom
FÜR NOVEMBER 2018

Praxisbeispiel

# Live-Hacking mit Phishing

LISA LEICHTSINNIG KLICKT AUF EINE E-MAIL….

# E-Mail / Phising

Eine gute Methode zur kritischen Bewertung eingehender Nachrichten ist der **3-Sekunden-Sicherheits-Check** des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

1. Kenne ich den Absender?
2. Ergeben Betreff und Nachricht einen Sinn?
3. Habe ich einen Anhang von dieser Person erwartet?
4. **NICHT** auf einen Link klicken, sondern gezielt über den Browser die URL / Shop öffnen

**Grundsätzlich gilt**: Wer nichts macht – macht nichts verkehrt.

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

**SCHWACHSTELLE** | GEFÄHRDUNG | VORFALL | IT-ASSETS

# Aktive Ausnutzung einer Zero-Day Schwachstelle in Microsoft Office

*CSW-Nr. 2023-248752-1232, Version 1.2, 09.08.2023*

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten

**Weiter Praxisbeispiele von der KZV : https://bit.ly/praxis-sicherheit**

# Wichtige Fragen

# Wichtige Fragen (1)

**Mit welchem Aufwand ist bei der Umsetzung zu rechnen?**

- Die IT-Sicherheitsrichtlinie regelt weitestgehend das, was den Praxen auf durch die DSGVO und BDSG bereits vorgeschrieben wird. Der zusätzliche Aufwand zur Erfüllung der Vorgaben der IT-Sicherheitsrichtlinie dürfte für die meisten Praxen somit vergleichsweise gering sein.

**Sind Kontrollen in Form von Audits oder Praxisbegehungen vorgesehen?**

- Nein, aktuell sind keine Kontrollen in Praxen zur Überprüfung der IT-Sicherheit vorgesehen.

# Wichtige Fragen (2)

**Ab wann ist die IT-Sicherheitsrichtlinie für Zahnarztpraxen verbindlich?**

- Die Neufassung tritt am **2. Juli 2025** in Kraft. Neu eingeführte oder inhaltlich geänderte Anforderungen treten nach einer Übergangsfrist von sechs Monaten am **2. Januar 2026** in Kraft.

**Wer trägt die Verantwortung für die Datensicherheit in der Zahnarztpraxis?**

- Die Verantwortung für die Datensicherheit der Praxis-IT liegt zunächst beim Praxisinhaber.

# Wichtige Fragen (3)

**Welche Saktionen gibt es, wenn die Vorgaben der IT-Sicherheitsrichtlnie nicht eingehalten werden?**

- Die im SGB V verankerte gesetzliche Grundlage der IT-Sicherheitsrichtlinie (§ 390 SGB V) sieht derzeit keine eigenen Sanktionen vor. Die Richtlinie definiert Maßnahmen, die die Einhaltung der verschiedenen rechtlichen Vorgaben unterstützen.

**Gerade die DSGVO hat den Behörden die Möglichkeit gegeben, hohe Strafen durchzusetzen und auch im Straf- und Berufsrecht sind entsprechende Sanktionen vorgesehen.**

# Was ist in der Zahnarztpraxis zu tun?

1. **Einarbeitung und Ausscheiden von Mitarbeitern regeln,**
   - z.B. über Checklisten (A1-01 /A1-02)
2. **Fremdpersonal: Vertraulichkeitsvereinbarung erstellen (A1-03/04)**
   - Muster verfügbar unter: https://compfair.de/muster.zip
3. **Aufgaben und Zuständigkeiten festlegen (A1-05)**
4. **Durchführung von Schulung zur IT ( A1-10)**
5. **Praxisleitung sensibilisieren (A1-08)**
6. **REST: IT-Dienstleister: Regeln, Beauftragen, Überwachen**
   - **Datensicherung nicht vergessen ;-)**

Weitere Informationen unter: https://bit.ly/kzbv-it

# Vielen Dank!

P.S Datensicherung machen ;-)

Rückfragen / Anmerkung gerne an:
Richard Marnau marnau@compfair.de