Verein für Technische & Digitale Resilienz (VTDR) i. G.

Empirische Analyse der IT-Sicherheitslage deutscher Arztpraxen im Kontext Cybersicherheitslage in Deutschland

Forschungsprojekt KRITIS-3.0-Framework

Ronny Woick
Information Security Officer (certified) & IT-Berater
Verein für Technische & Digitale Resilienz (VTDR) i. G.

E-Mail: r.woick@vtdr.de
Web: https://vtdr.de/
Telefon: +49 176 829 63 295

Executive Summary

Diese wissenschaftliche Arbeit untersucht den aktuellen Stand der IT-Sicherheit am Beispiel der deutschen Arztpraxen. Mittels des eigens entwickelten KRITIS-3.0-Frameworks wurden **1.391 Domains** analysiert, von denen **706 (50,8 %)** als verwundbar eingestuft wurden.

Die Studie identifiziert strukturelle Schwachstellen in Wartung, Update-Praxis und Konfigurationshärtung. Im Gegensatz zu Apotheken unterliegen Hausarztpraxen derzeit keiner NIS2-Compliance-Pflicht, was die identifizierten Schwachstellen jedoch nicht weniger kritisch macht. Die Risiken reichen von **Ransomware-Erpressung** über **Phishing-Angriffe** und **Patientendatendiebstahl** bis hin zu **existenzbedrohenden Praxisausfällen**.

Die Erkenntnisse dieser Forschungsarbeit gewinnen zusätzliche Relevanz angesichts der aktuellen IT-Sicherheitslage in Deutschland. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt die Situation in seinem Lagebericht 2024 als **"besorgniserregend"**. Insbesondere kleine und mittlere Unternehmen – zu denen auch Hausarztpraxen zählen – sind von Ransomware-Angriffen betroffen und weisen oftmals unzureichende Sicherheitsvorkehrungen auf.

1. Forschungsziel und Relevanz

1.1 Zentrale Forschungsfrage

Wie ist der aktuelle Stand der IT-Sicherheit in der Arztbranche und welche konkreten Bedrohungsszenarien ergeben sich aus verwundbaren Praxis-Websites?

1.2 Wissenschaftliche und gesellschaftliche Relevanz

Die Studie leistet einen Beitrag zur empirischen Cyber-Sicherheitsforschung durch:

- Quantitative Erhebung des IT-Sicherheitsstatus einer gesamten Branche
- Identifikation von Schwachstellenmustern
- Entwicklung praxisnaher Handlungsempfehlungen für Betreiber und Verbände
- **Dokumentation realer Angriffsszenarien** auf Basis aktueller Vorfälle im Gesundheitswesen

Arztwebsites sind Teil der Versorgungsinfrastruktur und verarbeiten teilweise sensible Gesundheitsdaten. Kompromittierte Systeme können:

- **Vertrauen von Patienten nachhaltig beschädigen**
- **Phishing-Kampagnen im Gesundheitssektor ermöglichen**
- **Patientendaten gefährden und dem Darknet zuführen**
- **Den Praxisbetrieb existenzbedrohend lahmlegen**

Die Studie trägt zur Verbesserung der Cyber-Resilienz im Gesundheitswesen bei.

2. Methodik

2.1 KRITIS-3.0-Framework

Die Untersuchung basiert auf einer **passiven automatisierten Sicherheitsanalyse** mittels des eigens entwickelten KRITIS-3.0-Frameworks. Das Framework ermöglicht eine quantitative Bewertung der IT-Sicherheitslage durch:

- **Netzwerk- und TLS-Analyse**: Erkennung unsicherer Protokolle und Zertifikatsfehler
- **CMS- und Komponentenprüfung**: Abgleich gegen bekannte Schwachstellen
- **Clientseitige JavaScript-Analyse**: Identifikation veralteter Bibliotheken
- **OSINT-Integration**: Nutzung von CVE/NVD-Datenbanken
- **Risiko-Scoring**: Aggregierte Indikatoren
- **Revisionssicheres Audit-Logging**: Nachvollziehbarkeit aller Analysen

Wichtig: Es wurden **keine aktiven Penetrationstests** durchgeführt. Die Analyse beschränkte sich auf öffentlich zugängliche Informationen (HTML, CSS, JavaScript, HTTP-Header, DNS-Einträge), um die Integrität der untersuchten Systeme zu gewährleisten und ethischen Standards zu entsprechen.

Scan-Dauer: 150–300 Sekunden pro Domain

2.2 Erhobene Metriken

Das Framework bewertet folgende Kernmetriken:

Metrik	Beschreibung
DVI	Domain Vulnerability Index: Relatives Gesamtrisiko der Domain (0–10)
ESS	Exposed Services Score: Umfang exponierter Dienste (APIs, Debug-Schnittstellen)
CAR	Component Age Risk: Alter kritischer Komponenten (0–10)
ASS	Attack Surface Score: Relative Angriffsfläche
SHD	Security Header Deficit: Anzahl fehlender HTTP-Sicherheitsheader (0–6)
CVSS-Zeitdifferenz	Tage zwischen CVE-Publikation und Scan-Zeitpunkt

2.3 Stichprobe

1.391 Domains von Hausarztpraxen (mit Varianten von "hausarzt.de", "hausarzt-*.de", "praxis-*.de" und ähnlichen Mustern) wurden vollautomatisiert mittels passiver Analyse untersucht.

2.4 Komponentenverteilung

- **WordPress-Komponenten**: 929
- **JavaScript-Komponenten**: 451
- **Andere Systeme**: 0

3. Zentrale Ergebnisse

3.1 Gesamtübersicht

706 von 1.391 Domains (50,8 %) wurden als verwundbar eingestuft.

685 Domains zeigten keine erkennbaren Schwachstellen. Diese hohe Verwundbarkeitsrate liegt deutlich über dem erwartbaren Niveau.

3.2 Aggregatmetriken (alle Domains, n = 1.391)

Hinweis: Werte basieren auf allen 1.391 Domains; nicht-verwundbare Domains haben Risiko-Werte von 0.

Metrik	Mittelwert	Median	90-Perzentil
DVI	1,09	**0,50**	3,00
ESS	2,16	**1,50**	5,50
SHD (fehlende Header)	5,39	**6,00** ⚠	6,00
CAR	3,39	**0,00**	**10,00** ⚠
ASS	3,10	**2,80**	5,00
Max. CVE-Zeitdiff. (Tage, n=632)	1.184	**886** ⚠	**2.484** ⚠
Ø CVE-Zeitdifferenz (Tage)	761	**505**	**2.385** ⚠

Interpretation

(1) SHD nahe am Maximum (Median **6**) weist auf **systematische Header-Härtungsdefizite** hin.

(2) CAR ist stark **rechtsschief** (Median 0, P90 = 10) → viele Seiten aktuell, aber ein großer **Anteil veralteter Komponenten**.

(3) CVE-Zeitdifferenzen belegen **lange Patch-Latenzen** bis in den Mehrjahresbereich.

3.3 Schweregradverteilung der Schwachstellen

Von den **706 verwundbaren Domains**:

Schweregrad	Anzahl	Prozent
Kritisch	**78**	11,0 %
Hoch	**145**	20,5 %
Mittel	**437**	61,9 %
Niedrig	**46**	6,5 %

Die Verteilung zeigt eine Dominanz mittelgradiger Schwachstellen (437), jedoch sind **223 Funde (kritisch + hoch)** sicherheitsrelevant im Sinne potenzieller Ausnutzbarkeit.

3.4 Komponenten und Angriffspfade

- **CMS/Plugins (WordPress)**: Haupttreiber der Befunde (insb. Formular-, Builder-, Medien- und SEO-Plugins)
- **JavaScript-Ökosystem**: Bibliotheken/Loader, veraltete Framework-Artefakte; potenziell XSS/Info-Disclosure
- **Sicherheitsheader**: häufig fehlend: HSTS, CSP, X-Content-Type-Options, X-Frame-Options, Referrer-Policy, Permissions-Policy

4. Konkrete Risiken bei kompromittierten Hausarzt-Websites

4.1 Ransomware-Angriffe und Existenzbedrohung

Reales Szenario aus München

https://cybercheck.de/cyber-blog/protokoll-eines-hackerangriffs-auf-eine-arztpraxis

Ein Allgemeinmediziner mit 10-köpfigem Praxis-Team wurde Opfer eines Krypto-Trojaners. Die gesamte Praxis-EDV war betroffen:

- Patientendaten
- Röntgenbilder und Ultraschallaufnahmen
- Sensible Arztbefunde
- Finanzbuchhaltung
- E-Mail-Server

Folgen:

- Keine Dateien ließen sich mehr öffnen
- Normaler Praxisbetrieb unmöglich
- Lösegeldforderung in Bitcoin
- IT-Dienstleister konnte binnen 45 Minuten vor Ort nichts ausrichten
- **Situation wurde als "absolut existenzbedrohend" eingestuft**

Der Arzt musste letztlich das Lösegeld bezahlen, um die Praxis-IT zurückzubekommen.

4.2 Patientendatendiebstahl und Darknet-Handel

Warum Patientendaten besonders wertvoll sind

Patientendaten erzielen im **Darknet häufig höhere Preise** als Bank- und Kontoinformationen, da sie:

- Hochsensible Gesundheitsinformationen enthalten
- Für Identitätsdiebstahl nutzbar sind
- Erpressungspotenzial bieten (z.B. bei peinlichen Diagnosen)
- Versicherungsbetrug ermöglichen

Datentypen, die gefährdet sind:

- Name, Adresse, Geburtsdatum
- Krankenversicherungsnummer
- Behandlungsgrund und Diagnosen
- Medikationen
- Terminhistorie (welcher Facharzt wann aufgesucht wurde)
- Kontodaten für Privatpatienten

4.3 Phishing und Social Engineering

Kompromittierte Websites als Sprungbrett

Verwundbare Hausarzt-Websites werden genutzt für:

1. **Fake-Terminbuchungsformulare**
    - Sammeln von Patientendaten unter dem Deckmantel seriöser Terminvereinbarung
    - Weiterleitung zu Phishing-Seiten
2. **E-Mail-Phishing mit vertrauenswürdigem Absender**
    - Kompromittierte Praxis-E-Mail-Accounts
    - Versand von Schadsoftware an Patienten
    - "Rechnung für Privatleistung" als Köder

3. **Malware-Distribution**
    - Drive-by-Downloads beim Besuch der Website
    - Infizierung von Patienten-PCs
    - Weitere Verbreitung in deren Netzwerken

4.4 Online-Terminbuchungsportale als Schwachstelle

Dokumentierte Sicherheitslücken

Im Sommer 2020 wurde eine gravierende Sicherheitslücke bei einem großen Terminbuchungsportal bekannt:

- **Zugriff auf Millionen Terminvereinbarungen** inklusive Arzt- und Patientendaten
- Terminvereinbarungen **bis in die 1990er-Jahre** waren abrufbar
- Betroffene Daten:
    - Patientenname
    - Termingrund (= Gesundheitsinformation!)
    - Arztpraxis (gibt Rückschlüsse auf Erkrankung)
    - Zeitpunkt des Besuchs

Datenschutzproblematische Praktiken

Aktuelle Kritik an Terminportalen:

- **Excessive Datensammlung**: Anbieter fordern mehr Daten an als für Terminbuchung nötig
- **Verknüpfung mit Praxisdaten**: Bei Cyberangriff auf Portal sind auch interne Praxisdaten betroffen
- **Unklare Verantwortlichkeiten**: Praxisinhaber bleiben verantwortlich, auch wenn Portal gehackt wird
- **KI-Training mit Patientendaten**: Einige Anbieter nutzen anonymisierte Daten für KI-Modelle

4.5 Rechtliche und finanzielle Folgen

DSGVO-Verstöße und Bußgelder

Bei Datenpanne drohen:

- **Meldepflicht** an Aufsichtsbehörde binnen **72 Stunden**
- **Benachrichtigung** aller betroffenen Patienten
- **Bußgelder** bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes
- **Schadenersatzforderungen** von Patienten

Weitere finanzielle Schäden

- **Betriebsunterbrechung**: Keine Einnahmen während IT-Ausfall
- **IT-Notfallwiederherstellung**: Kosten für externe IT-Spezialisten
- **Lösegeldzahlung**: Falls entschieden wird zu zahlen (wird aber abgeraten)
- **Reputationsschaden**: Patientenverlust durch Vertrauensverlust
- **Erhöhte Versicherungsprämien**: Cyberversicherungen werden teurer oder lehnen ab

Strafrechtliche Risiken

- **§ 203 StGB (Verletzung von Privatgeheimnissen)**: Bei unzureichendem Schutz von Patientendaten
- **Persönliche Haftung** der Praxisinhaber
- **Organisationsverschulden**: Bei fehlenden IT-Sicherheitsmaßnahmen

4.6 Vertrauensverlust und Praxisreputation

Langfristige Auswirkungen

- **Medienberichterstattung**: Lokale Presse berichtet über Datenpannen
- **Mundpropaganda**: Patienten warnen einander
- **Online-Bewertungen**: Negative Rezensionen auf jameda, Google etc.
- **Patientenabwanderung**: Wechsel zu als sicherer wahrgenommenen Praxen

Besonders sensible Fachbereiche

Kompromittierungen sind besonders kritisch bei:

- Psychotherapeuten (stigmatisierte Erkrankungen)
- Hautärzten (ästhetische Behandlungen)
- Urologen/Gynäkologen (intime Probleme)
- Kinderwunschzentren (persönliche Lebensplanung)

4.7 Manipulation medizinischer Geräte (bei Vernetzung)

Bei vernetzten Praxissystemen drohen:

- **Manipulation von Behandlungsgeräten**: Moderne Geräte mit Netzwerkanbindung
- **Verfälschung von Befunden**: Wenn Bildgebung kompromittiert wird
- **Gefährdung der Patientengesundheit**: Bei kritischen Systemen

5. Diskussion

Die Ergebnisse zeichnen ein **duales Risikoprofil**:

(a) Akute Hochrisiken (kritisch/hoch) in einem substantiellen Teil der Stichprobe
(b) Breite Strukturdefizite (v.a. Header-Härtung, Patch-Latenz) über die Hälfte der Grundgesamtheit

Die starke Abhängigkeit vom **CMS-Ökosystem** macht **Patch-Management, Inventarisierung und Testprozesse** zu zentralen Steuerungshebeln. Die Metriken zeigen konsistent: **Schnelle Quick-Wins** (Header, Deaktivierung/Update einzelner Plugins) können das Niveau rasch erhöhen; **Governance-Maßnahmen** sichern die Nachhaltigkeit.

Besonderheit: Keine NIS2-Pflicht, aber reale Bedrohungen

Anders als Apotheken ab bestimmter Größe sind Hausarztpraxen **nicht NIS2-pflichtig**. Dies bedeutet jedoch nicht, dass die Bedrohungslage geringer wäre:

- **Cyberkriminelle unterscheiden nicht** nach regulatorischem Status
- **Patientendaten sind hochwertig** unabhängig von der Einrichtungsgröße
- **Praxisausfälle haben direkte Versorgungsfolgen** für Patienten
- **Reputationsschäden wirken existenzbedrohend** auch ohne Bußgelder

Die **Eigenverantwortung** der Praxisinhaber ist daher umso höher.

6. Limitationen

- **Passiver Ansatz**: Keine Verifikation durch Exploitation; mögliches Under-/Over-Reporting bei Versions-Heuristiken
- **Sichtbarkeitsbias**: Nur öffentlich erreichbare Artefakte; interne Schutzmechanismen bleiben unbewertet
- **Zeitpunktbezogen**: Befunde spiegeln den Erhebungszeitraum; dynamische Änderungen sind möglich
- **Website ≠ Praxis-IT**: Die Website-Sicherheit gibt nur bedingt Aufschluss über die interne IT-Infrastruktur

7. Empfehlungen (priorisiert)

7.1 Sofortmaßnahmen

1. Kritische/Hohe Befunde priorisiert beheben

- Update/Removal verwundbarer Plugins/Themes
- Notfall-Patches einspielen
- Besonderer Fokus auf RCE-Schwachstellen (Remote Code Execution)

2. Sicherheitsheader vollständig aktivieren

- Content-Security-Policy (CSP)
- HTTP Strict Transport Security (HSTS)
- X-Frame-Options
- X-Content-Type-Options
- Referrer-Policy
- Permissions-Policy
- *(Inkl. Test in Staging-Umgebung)*

3. Formularpfade härten

- TLS-Erzwingung (HTTPS überall)
- CSRF-Schutz (Cross-Site Request Forgery)
- Minimaldatenerhebung (nur nötigste Felder)
- Logging auf Fehlkonfigurationen
- **Captcha bei Kontaktformularen**

7.2 Strukturelle Maßnahmen

4. Komponenten-Inventar etablieren

- Vollständige Liste: Quelle/Version/Supportstatus
- Patch-Kalender mit Verantwortlichkeiten
- Automatische Update-Benachrichtigungen

5. Technische Schulden abbauen

- Legacy-JavaScript entfernen
- Ungenutzte Plugins/Theme-Reste deinstallieren
- Obsolete Funktionalitäten stilllegen

6. Regelmäßiges Monitoring

- Monatliche passive Scans mit KRITIS-Metriktracking
- Quartalsweise Security-Reviews
- Kontinuierliches Vulnerability-Management

7. Online-Terminportale kritisch prüfen

- Datenschutzkonforme Anbieter wählen
- Auftragsverarbeitungsverträge (AVV) prüfen lassen
- Keine exzessive Datenweitergabe akzeptieren
- Widerspruchsmöglichkeiten für Patienten schaffen

7.3 Governance & Betrieb

8. Verantwortlichkeiten definieren

- Klare Zuordnung: Praxis / Agentur / Hoster
- Eskalationspfade festlegen
- Notfallkontakte dokumentieren

9. Nachvollziehbarkeit/Dokumentation

- Änderungsprotokoll (Patches, Updates)
- Test-Dokumentation
- Nachweisführung für DSGVO-Compliance

10. Sensibilisierung und Schulung

- Kurzleitfäden für Praxisteams
- Webinare zu: Header, Patches, Formularsicherheit
- Phishing-Awareness-Training
- Jährliche Auffrischung

11. Notfallplan erstellen

- **Was tun bei Ransomware-Angriff?**
    - IT-Systeme vom Netz trennen
    - IT-Dienstleister/Experten kontaktieren
    - Polizei einschalten (Strafanzeige)
    - Datenschutzbehörde informieren (72h)
    - Beweise sichern
    - **Kein Lösegeld zahlen** (Empfehlung der Behörden)
- **Backup-Strategie** (3-2-1-Regel)
    - 3 Kopien der Daten
    - 2 verschiedene Speichermedien Kopie offline/offsite

12. Cyberversicherung prüfen

- Kosten-Nutzen-Abwägung
- Deckungsumfang genau prüfen
- Beachtung: Hohe Prämien/Ablehnungen im Gesundheitswesen
- Dokumentationspflichten für Versicherer erfüllen

8. Schlussfolgerung

Rund **jede zweite** untersuchte Hausarzt-Website weist verwundbare Befunde auf. Neben **akut priorisierungsbedürftigen** Fällen (kritisch/hoch) dominiert ein **breites, aber gut adressierbares Strukturproblem** (Header-Härtung, Patch-Latenz, Komponenten-Altlasten).

Realen Angriffsszenarien zeigen:

- **Ransomware-Angriffe** können existenzbedrohend sein
- **Patientendaten** sind hochwertige Beute im Darknet
- **Phishing** über kompromittierte Praxis-Websites gefährdet Patienten
- **Reputationsschäden** und **rechtliche Konsequenzen** sind schwerwiegend

Konsequente **Sofortmaßnahmen** und **Governance-gestütztes** Lifecycle-Management senken das Risiko messbar – im Sinne der KRITIS-3.0-Leitplanken und zum Schutz der Patientenversorgung.

Call to Action

Für Praxisinhaber:

- Sofortige IT-Sicherheitsevaluierung durchführen
- Kritische Schwachstellen binnen 30 Tagen beheben
- Notfallplan erstellen und testen

Für Verbände:

- Branchenspezifische Leitfäden entwickeln
- Zentrale Anlaufstelle für Sicherheitsfragen schaffen
- Schulungsangebote ausbauen

Für Politik/Behörden:

- Freiwillige Sicherheitsinitiativen fördern
- Niedrigschwellige Beratungsangebote schaffen
- Best-Practice-Austausch ermöglichen

9. Anhang (Kennzahlenüberblick)

- **Grundgesamtheit**: 1.391 Domains
- **Verwundbar**: 706 (50,8 %) – **Ohne Befund**: 685 (49,2 %)
- **Schweregrade** (n = 706): kritisch **78** | hoch **145** | mittel **437** | niedrig **46**
- **Komponenten**: WordPress-bezogen **929** | JavaScript-bezogen **451**
- **KRITIS-Metriken** (Median): DVI **0,5** | ESS **1,5** | SHD **6** | CAR **0** | ASS **2,8**
- **CVE-Zeitdifferenzen** (Median/90-P): **886 / 2.484 Tage**

Verein für Technische & Digitale Resilienz (VTDR) i. G.

10. Kontakt und Kooperation

Verfasser

Ronny Woick
Information Security Officer (certified) & IT-Berater
Verein für Technische & Digitale Resilienz (VTDR) i. G.

✉ E-Mail: r.woick@vtdr.de
🌐 Web: https://vtdr.de/
📞 Telefon: +49 176 829 63 295

Zweck: Förderung der IT-Sicherheit und digitalen Resilienz durch Forschung, Aufklärung und Entwicklung gemeinwohlorientierter Analysetools.

Der Verein verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke im Sinne der §§ 51 ff. AO. Es erfolgt keine Gewinnerzielung; sämtliche Einnahmen dienen der Erfüllung des Vereinszwecks.

Datenerhebung: Die Analysen beschränkten sich ausschließlich auf öffentlich erreichbare Webinhalte (z. B. HTML-, CSS- und JavaScript-Dateien) sowie standardisierte HTTP-Header. Es wurden keine geschützten Bereiche aufgerufen, keine Authentifizierungsmechanismen umgangen und keine aktiven Penetrationstests durchgeführt.

Kooperationsmöglichkeiten

- **Behörden (BSI, LKA)**: Datenaustausch und Koordination
- **Praxispartner**: Pilotprojekte zur Härtung
- **Forschungseinrichtungen**: Gemeinsame Publikationen
- **Verbände**: Best-Practice-Entwicklung
- **Kassenärztliche Vereinigungen**: Schulungs- und Beratungsangebote

Quellen

Die Analyse basiert auf:

- KRITIS-3.0-Frameworks Auswertung
- CVE/NVD-Datenbanken
- Dokumentierten Realtfällen aus Fachpublikationen
- BSI-Lagebericht 2024
- Forschung zu Datenpannen bei Online-Terminportalen (CCC 2020)
- Datenschutzbehörden-Berichten

Dokument erstellt: November 2025