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

Empirische Analyse der IT-Sicherheitslage deutscher Apotheken im Kontext kritischer Infrastrukturen

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 in kritischen Infrastrukturen am Beispiel der deutschen Apothekenbranche. Mittels des eigens entwickelten KRITIS-3.0-Frameworks wurden **1.159 Domains** analysiert, von denen **758 (65,4 %)** als verwundbar eingestuft wurden. Die Studie identifiziert strukturelle Schwachstellen in Wartung, Update-Praxis und Konfigurationshärtung und liefert empirische Evidenz für die Notwendigkeit verbesserter Cyber-Resilienz-Maßnahmen – insbesondere vor dem Hintergrund der bevorstehenden NIS2-Anforderungen.

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"**. BSI-Präsidentin Claudia Plattner betont: "Die IT-Bedrohungslage ist weiterhin angespannt und das ist und bleibt besorgniserregend." Insbesondere kleine und mittlere Unternehmen sind von Ransomware-Angriffen betroffen und weisen oftmals unzureichende Sicherheitsvorkehrungen auf.

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

1. Forschungsziel und Relevanz

1.1 Zentrale Forschungsfrage

Wie ist der aktuelle Stand der IT-Sicherheit in der Apothekenbranche und welche Handlungsbedarfe ergeben sich durch die NIS2-Richtlinie?

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 in kritischen Infrastrukturen
- Entwicklung praxisnaher Handlungsempfehlungen für Betreiber und Regulierungsbehörden
- Aufzeigen der Dringlichkeit von Maßnahmen im Hinblick auf NIS2-Compliance

Apothekenwebsites sind Teil der kritischen Versorgungsinfrastruktur und verarbeiten teilweise sensible Gesundheitsdaten. Kompromittierte Systeme können Vertrauen beschädigen, Phishing-Kampagnen im Gesundheitssektor ermöglichen und Patientendaten gefährden. 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

1.159 Domains mit den Mustern "apotheke.de" und "apotheke-*" wurden vollautomatisiert mittels passiver Analyse untersucht.

2.4 Komponentenverteilung

- **WordPress-Komponenten:** 976
- **JavaScript-Komponenten:** 236
- **Andere Systeme:** 0

3. Zentrale Ergebnisse

3.1 Gesamtübersicht

758 von 1.159 Domains (65,4 %) wurden als verwundbar eingestuft.

401 Domains zeigten keine erkennbaren Schwachstellen. Diese hohe Verwundbarkeitsrate liegt deutlich über dem erwartbaren Niveau für kritische Infrastrukturen.

3.2 Aggregatmetriken (nur verwundbare Domains, n = 758)

Metrik	Mittelwert	Median	Minimum	Maximum	Std.abw.
Domain Vulnerability Index (DVI)	**1,75**	**1,00**	0,5	10,0	1,43
Exposed Services Score (ESS)	**2,59**	**1,50**	−0,5	7,5	2,21
Component Age Risk (CAR)	**8,35**	**10,00**	0,0	10,0	3,52
Attack Surface Score (ASS)	**3,38**	**2,67**	0,2	8,2	1,45
Security Header Deficit (SHD)	**4,91**	**5,00**	0,0	6,0	1,35
Ø CVSS-Zeitdifferenz (Tage)	**695**	**604**	3	3.104	523
Max. CVSS-Zeitdifferenz (Tage)	**937**	**604**	3	4.105	704

Interpretation:

Die Mehrzahl der Domains weist ein niedriges bis moderates Risikoniveau auf (DVI ≈ 1–2). Einzelne Ausreißer (DVI = 10,0) zeigen jedoch extreme Verwundbarkeit. Das durchschnittliche Komponentenalter (CAR = 8,35) und der Median von 10,0 verdeutlichen ein **strukturelles Patch-Defizit**. Fehlende Sicherheitsheader (SHD = 4,91 von 6) sind weit verbreitet. Die durchschnittliche Patch-Latenz von **695 Tagen** ist besorgniserregend.

3.3 Schweregradverteilung der Schwachstellen

Schweregrad	Anzahl
Kritisch	**74**
Hoch	**104**
Mittel	**557**
Niedrig	**23**

Die Verteilung zeigt eine Dominanz mittelgradiger Schwachstellen (557), jedoch sind **178 Funde (kritisch + hoch)** sicherheitsrelevant im Sinne potenzieller Ausnutzbarkeit.

3.4 Schwachstellentypen

Schwachstellentyp	Vorkommen
XSS (Cross-Site Scripting)	**143**
RCE (Remote Code Execution)	**18**
CSRF (Cross-Site Request Forgery)	**11**
SQL Injection	1
Path Traversal	0
Authentication Bypass	0
Information Disclosure	0
Denial of Service (DoS)	0

Schwachstellentyp	Vorkommen
Andere / unspezifisch	84

Analyse:

Das deutliche Übergewicht von **XSS-Schwachstellen (143 Fälle)** verweist auf unzureichende Eingabevalidierung und fehlende Content-Security-Policies (CSP). Die festgestellten **18 RCE-Fälle** stellen eine hohe Gefährdungslage dar, da sie meist vollständige Systemkompromittierung ermöglichen.

3.5 Häufig betroffene Komponenten

Komponente	Häufigkeit
js_composer	117
revslider	95
elementor / elementor-pro	91
layerslider	78
woocommerce	63
contact-form-7	57
mailpoet	46
rank-math	41
bootstrap	39
jquery	37

Interpretation:

Die meisten Schwachstellen sind auf **veraltete oder fehlerhafte WordPress-Plugins** zurückzuführen. Besonders betroffen sind visuelle Builder-Plugins und Slider-Komponenten, die häufig unsichere Skriptaufrufe oder veraltete Bibliotheken einbinden.

3.6 Beispielhafte Risikodomains (anonymisiert)

Domain	Max. Schweregrad	Gesamt-Schwachstellen	Max. CVSS	Wichtige Komponenten	DVI	ASS
Domain-A	Kritisch	86	10,0	elementor, give, swiper, bootstrap	6,5	4,8
Domain-B	Kritisch	44	9,9	widget-options, js_composer, jquery	10	8,2
Domain-C	Kritisch	20	9,8	give, woocommerce, mailpoet	6,0	6,6
Domain-D	Hoch	29	8,5	jet-engine, jet-popup, react, vue	10	8,2
Domain-E	Hoch	37	8,8	js_composer, revslider, gsap	7,0	6,6
Domain-F	Kritisch	29	9,8	layerslider, bridge, jquery	6,5	6,8

Diese anonymisierten Beispiele zeigen die typischen Risikoprofile: veraltete visuelle Page-Builder-Plugins, fehlende Sicherheitsheader und mehrere exponierte Dienste.

---

4. NIS2-Ausblick für Apotheken

4.1 Regulatorischer Rahmen

Die **NIS2-Richtlinie (EU) 2022/2555** wurde am 16. Januar 2023 wirksam und hätte bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden müssen. Deutschland hat diese Frist nicht eingehalten. Das **NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)** wird voraussichtlich im **Herbst 2025** in Kraft treten.

Rund **29.500 Unternehmen** in Deutschland werden von der Richtlinie betroffen sein, so BSI-Präsidentin Claudia Plattner.

4.2 Betroffene Apotheken

Kategorie	Schwellenwerte
Wichtige Einrichtungen	50–249 Mitarbeitende ODER • Weniger als 50 Mitarbeitende, aber mind. 10 Mio. EUR Jahresumsatz UND mind. 10 Mio. EUR Jahresbilanzsumme
Besonders wichtige Einrichtungen	Mind. 250 Mitarbeitende ODER • Mind. 50 Mio. EUR Jahresumsatz UND mind. 43 Mio. EUR Jahresbilanzsumme
Betreiber kritischer Anlagen	Apotheken mit mind. 4.650.000 abgegebenen Packungen pro Jahr

Ergänzend zu den genannten Schwellenwerten ist zu beachten, dass diese nur für Einrichtungen gelten, die in einem der durch das NIS2-Umsetzungs- und das BSI-Gesetz definierten Sektoren tätig sind – etwa Energie, Verkehr, Gesundheit, Wasser oder Informations- und Kommunikationstechnologie. Neben der Unternehmensgröße (Mitarbeitende, Umsatz, Bilanzsumme) können in bestimmten Bereichen zusätzlich spezifische technische oder mengenbezogene Schwellenwerte greifen, etwa die Zahl abgegebener Arzneimittelpackungen bei Apotheken. Sobald eine Einrichtung als „wichtig“ oder „besonders wichtig“ eingestuft wird, bestehen Melde- und Registrierungspflichten gegenüber der zuständigen Behörde. Mit der Umsetzung der NIS2-Richtlinie ab 2025 wird der Kreis betroffener Einrichtungen zudem deutlich erweitert, weshalb eine regelmäßige Überprüfung der Einstufung empfohlen wird.

4.3 Kernpflichten für betroffene Apotheken

4.3.1 Registrierungspflicht

- Registrierung beim BSI **innerhalb von 3 Monaten** nach Inkrafttreten des Gesetzes
- Angabe von Name, Anschrift, relevanten Sektoren und Kontaktdaten
- BSI stellt ein Online-Tool zur Betroffenheitsprüfung bereit

4.3.2 Risikomanagement (§ 30 BSIG-neu)

Technische und organisatorische Maßnahmen nach **Stand der Technik**:

- Risikoanalyse und Sicherheitskonzepte
- Konzepte zur Bewältigung von Sicherheitsvorfällen
- Business Continuity Management
- Sicherheit in der Lieferkette
- Backup-Management und Wiederherstellungskonzepte
- Konzepte zum Einsatz von Verschlüsselung
- Zugangskontrolle und Multi-Faktor-Authentifizierung
- Regelmäßige Sicherheitsüberprüfungen und Audits
- Schulungen der Mitarbeitenden zu IT-Sicherheit

- Verwendung gesicherter Kommunikation

4.3.3 Meldepflichten (§ 32 BSIG-neu)

Dreistufiges Meldesystem bei erheblichen Sicherheitsvorfällen:

Stufe	Frist	Inhalt
Erstmeldung	**24 Stunden**	Unverzüglich nach Kenntniserlangung
Folgemeldung	**72 Stunden**	Bewertung der Schwere und Auswirkungen
Abschlussbericht	**1 Monat**	Ursachenanalyse und ergriffene Maßnahmen

4.3.4 Geschäftsleitungsverantwortung

- Die Geschäftsleitung trägt die **direkte Verantwortung** für die Einhaltung der Cybersicherheitsanforderungen
- Verpflichtende Teilnahme an Cyber-Security-Schulungen
- **Persönliche Haftung** bei Verstößen möglich
- Überwachung der Umsetzung der Maßnahmen

4.4 Sanktionen

Kategorie	Bußgeld
Wichtige Einrichtungen	Bis zu **7 Mio. EUR** oder **1,4 % des weltweiten Jahresumsatzes** (höherer Betrag maßgeblich)
Besonders wichtige Einrichtungen	Bis zu **10 Mio. EUR** oder **2 % des weltweiten Jahresumsatzes** (höherer Betrag maßgeblich)

Weitere Maßnahmen:

- Anordnungen zur Nachbesserung durch das BSI
- Vorübergehender Entzug von Genehmigungen

- Untersagung der Geschäftsführertätigkeit bei schwerwiegenden Verstößen

5. Zusammenhang zwischen aktueller Sicherheitslage und NIS2

5.1 Dringlichkeit der Ergebnisse

Die Studienergebnisse zeigen, dass **65,4 % der analysierten Apotheken-Domains verwundbar** sind. Dies steht in erheblichem Widerspruch zu den kommenden NIS2-Anforderungen:

Ist-Zustand	NIS2-Anforderung
92 % fehlt Content Security Policy	Stand-der-Technik-Sicherheitsmaßnahmen erforderlich
Durchschnittliche Patch-Latenz: 695 Tage	Zeitnahe Schwachstellenbehebung gefordert
18 % mit RCE-Schwachstellen	Erhebliche Sicherheitsvorfälle müssen binnen 24h gemeldet werden
68 % fehlt HSTS	Verschlüsselung und sichere Kommunikation verpflichtend
70 % mit veralteten Komponenten (CAR > 8)	Kontinuierliches Patch-Management erforderlich

5.2 Risikoabschätzung

Ohne umfassende Maßnahmen droht:

- Nichteinhaltung der NIS2-Pflichten bei Inkrafttreten
- Hohe Bußgelder (bis zu 10 Mio. EUR oder 2 % des weltweiten Umsatzes)
- Persönliche Haftung der Geschäftsleitung
- Reputationsschäden bei Sicherheitsvorfällen
- Versorgungsengpässe durch Cyberangriffe

Handlungsfenster: Die Zeit bis zum Inkrafttreten des NIS2UmsuCG (voraussichtlich Herbst 2025 / Anfang 2026) sollte genutzt werden, um die identifizierten Schwachstellen zu beheben.

---

6. Handlungsempfehlungen

6.1 Sofortmaßnahmen (unabhängig von der Betroffenheit)

1. Betroffenheitsprüfung durchführen

- BSI-Online-Tool nutzen: https://www.bsi.bund.de
- Mitarbeiterzahl, Umsatz und Bilanzsumme prüfen
- Bei Unsicherheit: Rechtliche Beratung einholen

2. IT-Sicherheitsstatus evaluieren

- Inventarisierung aller IT-Systeme und Komponenten
- Identifikation veralteter Software und Schwachstellen
- Überprüfung der Patch-Management-Prozesse

3. Quick Wins umsetzen

- Alle Software-Updates zeitnah installieren
- Sicherheitsheader implementieren (CSP, HSTS, X-Frame-Options)

- Multi-Faktor-Authentifizierung für alle Admin-Zugänge aktivieren
- Backup-Strategie etablieren (3-2-1-Regel)

6.2 Mittelfristige Maßnahmen (bis Inkrafttreten NIS2)

4. Informationssicherheits-Managementsystem (ISMS) aufbauen

- Orientierung an ISO 27001 oder BSI IT-Grundschutz
- Dokumentation aller Sicherheitsmaßnahmen
- Etablierung von Prozessen für Incident Response

5. Schulungen und Awareness

- Regelmäßige Sicherheitsschulungen für alle Mitarbeitenden
- Geschäftsleitung in Cyber-Security weiterbilden
- Simulationen von Phishing-Angriffen durchführen

6. Externe Unterstützung einbinden

- IT-Sicherheitsberater hinzuziehen
- Penetrationstests durch externe Dienstleister
- Prüfung der Cyberversicherung

6.3 Langfristige Maßnahmen (kontinuierliche Verbesserung)

7. Kontinuierliches Monitoring

- Implementierung von Security Information and Event Management (SIEM)
- Regelmäßige Schwachstellenscans
- Monitoring der IT-Sicherheitslage

8. Lieferkettenmanagement

- Überprüfung der IT-Sicherheit von Dienstleistern
- Vertragsklauseln zu Sicherheitsanforderungen

- Regelmäßige Audits von Lieferanten

6.4 Unterstützungsangebote

Bundesamt für Sicherheit in der Informationstechnik (BSI):

- Online-Betroffenheitsprüfung
- Leitlinien und Handreichungen
- #nis2know-Infopakete
- Geschäftsleitungsschulungen

Branchenverbände:

- ABDA (Bundesvereinigung Deutscher Apothekerverbände) bietet Dokumentenpakete zur IT-Sicherheit
- Apothekerkammern bieten regionale Unterstützung

Länderinitiative:

- NIS2-Anlaufstellen (z.B. in NRW) mit kostenfreier Erstberatung

---

7. Fazit und Ausblick

7.1 Zentrale Erkenntnisse

Die empirische Analyse der Apotheken-Domains zeigt eine **kritische Sicherheitslage**:

- **65,4 % der Systeme** sind verwundbar
- Patch-Latenzen von durchschnittlich **695 Tagen**
- Fehlende Sicherheitsheader (im Schnitt **4,9 von 6**)
- **18 RCE-Schwachstellen** mit kritischem Gefährdungspotenzial
- **143 XSS-Schwachstellen** durch unzureichende Eingabevalidierung

Das Gesamtergebnis weist auf **strukturelle Schwachstellen in Wartung, Update-Praxis und Konfigurationshärtung** hin.

7.2 Implikationen für die Cyber-Resilienz

1. **Etablierung kontinuierlichen Patch-Managements:** Automatisierte Update-Prozesse und regelmäßige Schwachstellen-Scans sollten verpflichtend werden
2. **Härtung der Webserver-Konfiguration:** Alle Systeme sollten die Sicherheitsheader Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy und Permissions-Policy implementieren
3. **Verwaltung von Drittkomponenten:** Kritische Plugins (z.B. Slider- oder Page-Builder-Module) sind durch geprüfte Alternativen zu ersetzen
4. **Monitoring und Incident-Response:** Einführung von kontinuierlicher Überwachung (24/7-Vulnerability-Monitoring) mit definierten SLAs zur Behebung kritischer CVEs innerhalb von 7 Tagen
5. **Schulung und Sensibilisierung:** Betreiber und Agenturen benötigen Schulungen zur sicheren Webentwicklung, insbesondere im Bereich Eingabevalidierung und Sicherheitsheader

7.3 Handlungsbedarf

Für Apotheken:

- Sofortige Evaluierung der IT-Sicherheit
- Zeitnahe Umsetzung von Basismaßnahmen
- Vorbereitung auf NIS2-Compliance

Für Verbände und Politik:

- Entwicklung branchenspezifischer Leitfäden
- Bereitstellung von Fördermitteln für IT-Sicherheit
- Aufbau von Unterstützungsstrukturen für KMU

Für Regulierungsbehörden:

- Begleitung der Transformation durch Beratungsangebote
- Angemessene Übergangsfristen
- Praxisnahe Umsetzungshilfen

7.4 Vision: Resiliente digitale Apothekenlandschaft

Langfristiges Ziel ist die Etablierung eines **kontinuierlichen Monitoring- und Verbesserungsprozesses** für die IT-Sicherheit kritischer Infrastrukturen:

- Automatisierte Schwachstellenerkennung
- Schnelle Benachrichtigung betroffener Organisationen
- Unterstützung bei der Härtung
- Regelmäßige Re-Evaluation

KRITIS 3.0 als Beitrag zur digitalen Souveränität:

- Unabhängigkeit von kommerziellen Sicherheitsdienstleistern
- Gemeinnütziger Ansatz ermöglicht Zugang für alle Organisationen
- Transparenz und wissenschaftliche Fundierung

Auch auf den Seiten der einzelner Landesverbände wurden dokumentierte Schwachstellen gefunden!

8. 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

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

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 beschränkte 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