ApoKonzept

Ist Ihre Apotheke beim nächsten Cyber-Angriff vorbereitet?

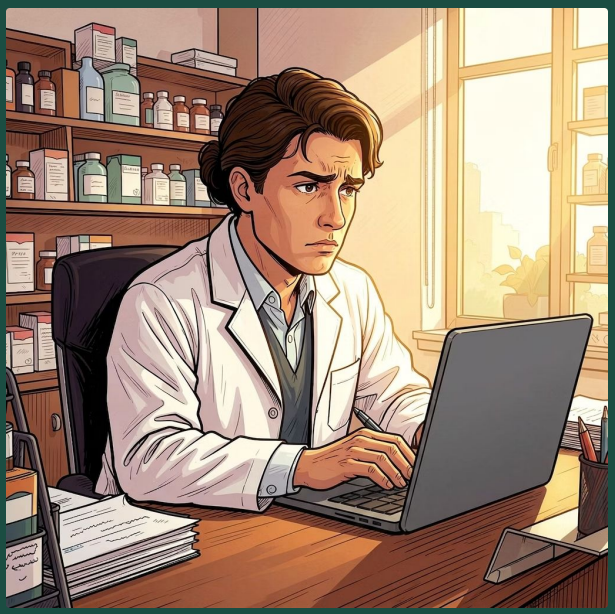
Der 15-Minuten-Check für Apothekeninhaber – 5 Lücken, die Sie heute kennen sollten, bevor der erste Schaden Ihre Existenz gefährdet.

Von Ioannis Trude & Benjamin Knors · ApoKonzept – Spezialisiert auf die Absicherung von Apotheken

EINLEITUNG

Warum Sie diese 15 Minuten investieren sollten

Stellen Sie sich vor: Es ist Montagmorgen, 8:15 Uhr. Sie schließen Ihre Apotheke auf. Der erste Kunde wartet schon mit einem E-Rezept auf dem Smartphone. Sie starten den Computer. **Nichts.** Das Warenwirtschaftssystem startet nicht. Die E-Rezept-Anbindung ist tot. Securpharm meldet Fehler. Ihr Telefon klingelt – ein Kunde fragt, warum seine Daten im Internet auftauchen.



So sieht ein Cyber-Angriff in einer deutschen Apotheke aus. Im Jahr 2026 ist das keine Ausnahme mehr.

Mein Name ist Ioannis Trude. Mit ApoKonzept habe ich mich darauf spezialisiert, Apotheken in ganz Deutschland 360 Grad abzusichern. In meinen Beratungsgesprächen sehe ich immer wieder dasselbe Muster: Beim Thema Cyber-Sicherheit gibt es bei fast jeder Apotheke gefährliche Lücken – Lücken, die im Schadenfall existenzbedrohend werden können.

In den nächsten 15 Minuten erfahren Sie:

- Warum Apotheken gerade jetzt im Fokus von Cyber-Kriminellen stehen
- Welche 5 Cyber-Lücken in fast jeder Apotheke vorhanden sind
- Welche 3 Sofortmaßnahmen Sie heute noch umsetzen können

So nutzen Sie dieses Dokument: Lesen Sie es in Ruhe durch. Gleichen Sie jeden Punkt mit Ihrer eigenen Apotheke ab. Machen Sie sich Notizen – die besprechen wir im Termin.

ApoKonzept

FALLBEISPIEL 2026

Der Unimed-Hack – Warum Apotheken gerade jetzt im Fokus stehen

Im April 2026 wurde der externe Abrechnungsdienstleister Unimed Opfer eines Cyber-Angriffs. Das Ergebnis: **Über 100.000 Patientendaten wurden gestohlen.**

Betroffen waren:

- Uniklinik Köln (30.000 Datensätze)
- UKE Hamburg (5.200 Fälle mit Gesundheits- und Finanzdaten)
- Universitätskliniken Freiburg, Ulm, Heidelberg, Tübingen (72.000 Betroffene)
- UKD Düsseldorf, Unimedizin Mainz, Uniklinikum Saarland

Diese Kliniken sind keine Amateure. Sie haben professionelle IT-Abteilungen, eigene Sicherheitsbeauftragte, sechsstellige IT-Budgets. Und trotzdem wurden sie über einen externen Dienstleister angegriffen.

Warum ist das für Sie als Apotheker relevant? Weil Sie genau die gleichen Risiken haben. Nur mit weniger Schutz.

ApoKonzept

BEDROHUNGSLAGE

Warum Apotheken attraktiv für Hacker sind

Apotheken sind für Hacker aus vier Gründen besonders attraktiv:

1. Sensible Gesundheitsdaten

Sie speichern Rezepte, Diagnosen, Krankenkassendaten, manchmal sogar BTM-Verschreibungen. Im Darknet werden solche Datensätze für **50 bis 250 Euro pro Person** gehandelt.

2. Finanzdaten

Sie rechnen mit Krankenkassen, Großhändlern und Lieferanten ab. Konto- und Vertragsdaten sind Gold wert.

3. Hochvernetzte Systeme

E-Rezept-Anbindung, Securpharm, Warenwirtschaft, Telematik-Infrastruktur. Je mehr Schnittstellen, desto mehr Einfallstore.

4. Mittlere IT-Reife, maximale Abhängigkeit

Die meisten Apotheken haben einen externen IT-Dienstleister – aber keinen eigenen Sicherheitsbeauftragten. Gleichzeitig steht der gesamte Betrieb still, sobald die Systeme ausfallen.

Ein realer Cyber-Schaden in einer Apotheke kostet schnell **50.000 bis 200.000 Euro**. Bei Datenschutzverletzungen kommen Bußgelder, Meldepflichten und Reputationsverluste dazu. Die gute Nachricht: Sie können das prüfen. In 15 Minuten. Mit diesem Dokument.

IRRTÜMER

Die 3 gefährlichen Irrtümer – Warum Standardlösungen nicht reichen

In meinen Gesprächen mit Apothekern höre ich immer wieder dieselben drei Sätze. Jeder davon ist ein gefährlicher Irrtum.

Der Hauptfehler: Die Annahme, dass Prävention allein ausreicht. Selbst die besten Systeme werden geknackt. Was wirklich schützt, ist die Kombination aus Prävention **UND** finanzieller Absicherung.

Irrtum 1: „Mein IT-Dienstleister kümmert sich darum."

Ihr IT-Dienstleister baut Firewalls, installiert Viren-Scanner und macht Updates. Das ist wichtig – aber es ist nur die halbe Miete. IT-Sicherheit verhindert Angriffe nicht zu 100 Prozent. Und wenn der Angriff durchkommt? Dann zahlt Ihr IT-Dienstleister nicht den Schaden. Er repariert das System. Den Rest tragen Sie.

Irrtum 2: „Wir sind zu klein, um interessant zu sein."

Das ist der gefährlichste Satz. Hacker greifen Apotheken nicht gezielt an. Sie verschicken Phishing-Mails an Zehntausende Adressen gleichzeitig. Wer klickt, wird Opfer – egal ob Konzern oder Drei-Mann-Apotheke.

Irrtum 3: „Meine Betriebshaftpflicht deckt das mit ab."

Tut sie in den meisten Fällen nicht. Klassische Policen schließen Cyber-Schäden faktisch aus oder decken nur kleine Teile. Wer hier nicht aktiv prüft, steht im Ernstfall ohne Schutz da.

Die 5 gefährlichsten Cyber-Lücken in Apotheken

	**Lücke 1 – E-Rezept-Ausfall & Warenwirtschaft**	Systemausfälle legen den Betrieb komplett lahm. Durchschnittliche Ausfallzeit bei Ransomware: **5–14 Tage**. Kosten: Umsatzausfall, Wiederherstellung – und Stammkunden, die zur Konkurrenz wechseln.
	**Lücke 2 – Patientendaten-Diebstahl**	Gestohlene Gesundheitsdaten lösen DSGVO-Meldepflicht, Bußgelder und Informationspflichten aus. Ein Vorfall mit 5.000 Betroffenen kostet schnell **80.000–150.000 Euro** – zuzüglich Vertrauensverlust.
	**Lücke 3 – CEO-Fraud & Fake-President**	Gefälschte E-Mails im Namen des Chefs verleiten Mitarbeiter zu Überweisungen. Klassische Versicherungen zahlen nicht. Typische Schadenssumme: **15.000–80.000 Euro**.
	**Lücke 4 – Erpressung & Ransomware**	Ein Klick verschlüsselt alle Systeme. Lösegeldforderungen: **20.000–150.000 Euro**. Ohne sauberes Backup nach der 3-2-1-Regel bleibt oft nur Zahlung oder Totalverlust.
	**Lücke 5 – Externe Dienstleister (das Unimed-Szenario)**	Wird Ihr Abrechnungsrechenzentrum oder Software-Anbieter gehackt, haften Sie als verantwortliche Stelle trotzdem nach DSGVO. Jeder externe Dienstleister ist ein potenzielles Einfallstor.

ApoKonzept

Sofort umsetzbar: Was Sie diese Woche tun können

Sie müssen nicht alle Lücken auf einmal schließen. Aber drei Schritte können Sie sofort gehen.

Maßnahme 1 – Backup-Check (heute)

Prüfen Sie, ob Ihre Datensicherung der **3-2-1-Regel** folgt. Drei Kopien, zwei verschiedene Medien, eine außer Haus. Wenn nicht: heute mit Ihrem IT-Dienstleister klären.

Maßnahme 2 – Mitarbeiter-Sensibilisierung (diese Woche)

Sprechen Sie im Team über Phishing-Mails und CEO-Fraud. Vereinbaren Sie ein verbindliches **Vier-Augen-Prinzip** bei allen Überweisungen ab einem festen Betrag.

Maßnahme 3 – Versicherungs-Check (zum Termin)

Legen Sie Ihre aktuellen Policen bereit. Wir prüfen gemeinsam, welche Cyber-Lücke aktuell gedeckt ist – und welche nicht.

Mini-Checkliste zum Abhaken:

- [ ] Backup läuft automatisch, mindestens wöchentlich
- [ ] Mitarbeiter wurden im letzten Jahr zu Cyber-Sicherheit geschult
- [ ] Es gibt einen Notfallplan für IT-Ausfall
- [ ] Aktuelle Versicherungspolicen liegen für den Termin bereit
- [ ] Liste externer Dienstleister mit Datenzugriff ist erstellt

ABSCHLUSS & KONTAKT

Was Sie im Termin erwartet

Cyber-Angriffe auf Apotheken sind keine Zukunftsmusik. Sie passieren jetzt. Die Frage ist nicht, ob – sondern wann. Und vor allem: ob Sie vorbereitet sind.

In unserem Termin (45 Minuten) bekommen Sie:

- Eine individuelle Risiko-Analyse für Ihre Apotheke
- Eine konkrete Absicherungs-Empfehlung – passend zu Größe und Struktur
- Eine klare Antwort: Welche Lücken haben Sie aktuell, was kostet die Schließung

Bitte zum Termin mitbringen:

- Aktuelle Versicherungspolicen (Betriebshaftpflicht, Inhalt, ggf. bestehende Cyber-Police)
- Übersicht Ihrer wichtigsten IT-Dienstleister
- Diese Checkliste mit Ihren Notizen

Ioannis Trude & Benjamin Knors | ApoKonzept

Generalagentur Ioannis Trude
Generalagentur Benjamin Knors
Robert-Perthel-Str. 77a · 50739 Köln

Kontakt

Telefon: +49 221 29240735
apokonzept@knors-trude.de
www.apokonzept.de

ApoKonzept