

NIS2 – Richtlinie: IT-Sicherheitsanalyse für Apotheken

Die EU-Richtlinie NIS2 stellt neue Anforderungen an die Cybersicherheit von Apotheken.

Wir unterstützen Sie dabei, die IT-bezogenen Sicherheitsrisiken zu erkennen und zu minimieren.



Cybersicherheit – das wichtige IT-Thema

IT-Sicherheit wird Pflicht: NIS2 und die Verantwortung für Ihre digitale Infrastruktur

Wo IT im Einsatz ist, muss auch an Cybersicherheit gedacht werden – das ist längst keine Option mehr, sondern Grundvoraussetzung für den sicheren Betrieb. Ohne eine tragfähige IT-Sicherheitsstrategie werden Digitalisierung, Automatisierung oder KI nicht zum Wettbewerbsvorteil, sondern zum potenziellen Risiko.

Gesetzgeber reagieren – Unternehmen stehen in der Pflicht

Dass viele Unternehmen, darunter auch Apotheken, noch unzureichend geschützt sind, zeigt die zunehmende Regulierung durch offizielle Stellen: EU-Parlament, Bundesregierung und BSI definieren klare Anforderungen an die IT-Sicherheit in Unternehmen – verbindlich und mit Fristen. Die Herausforderung: Betriebe müssen eigenständig prüfen, ob und in welchem Umfang sie betroffen sind – und zeitnah handeln.

Aktuell besonders relevant: Die NIS2-Richtlinie

Neben der DSGVO rückt nun die EU-Richtlinie **NIS2 (Network and Information Security 2)** in den Fokus. Sie löst die bisherige NIS1 ab, gilt für deutlich mehr Branchen – und verschärft die Anforderungen an IT-Sicherheit und Meldepflichten erheblich. Die Umsetzung in deutsches Recht erfolgt ab Oktober 2024 im Rahmen des sogenannten **IT-Sicherheitsgesetzes 3.0**.

Bin ich betroffen? Jetzt prüfen!

Die NIS2-Richtlinie betrifft mehr Unternehmen, als man zunächst vermuten würde – auch kleinere Apotheken und Betriebe können unter die Regelungen fallen. Ob Ihr Unternehmen dazu gehört, lässt sich einfach und schnell prüfen:

[Hier geht es zur offiziellen Betroffenheitsprüfung beim BSI](#)

Was bedeutet NIS2 konkret für Apotheken und Unternehmen?

Die NIS2-Richtlinie verpflichtet Apotheken und viele weitere Unternehmen dazu, ihre IT-Infrastruktur systematisch gegen potenzielle Bedrohungen abzusichern. Das betrifft alle Systeme, die für den täglichen Betrieb essenziell sind – von Warenwirtschaft über Rezeptabrechnung bis hin zu Kommunikationslösungen.

Insbesondere Apotheken, die als Teil des Gesundheitssektors unter die neue Gesetzgebung fallen können, müssen sicherstellen, dass ihre IT-Systeme zuverlässig vor Cyberangriffen geschützt sind.

Aber auch kleinere und mittlere Unternehmen geraten ins Visier der NIS2-Vorgaben: Wer in einem der betroffenen Sektoren tätig ist, sollte jetzt unbedingt die eigene Betroffenheit prüfen.

The background of the right side of the slide is a dark blue network of glowing nodes and connecting lines. The nodes are small circles in various colors (blue, orange, red) and are connected by thin, light-colored lines, creating a complex web-like structure. The text 'NIS2' is centered in the middle of this network.

NIS2

Unser Hinweis:

Ob Apotheke oder Herstellbetrieb – die NIS2-Richtlinie macht IT-Sicherheit zur gesetzlich geregelten Pflicht. Wir unterstützen Sie dabei, Ihre Systeme auf Herz und Nieren zu prüfen und die passenden Maßnahmen zu finden.



Unsere IT-Sicherheitsanalyse

Fokus:

Wir bieten Ihnen eine **gezielte Sicherheitsanalyse** an, die sich ausschließlich auf den **IT-Bereich** konzentriert. Dabei überprüfen wir Ihre IT-Infrastruktur und Sicherheitsvorkehrungen im Hinblick auf die Anforderungen der NIS2-Richtlinie.

Was wird analysiert?

- **Netzwerk- und Systemsicherheit:** Überprüfung der IT-Systeme auf Sicherheitsstand.
- **Datenschutz und Datenintegrität:** Sicherstellung des Schutzes Ihrer Kundendaten und relevanter Geschäftsinformationen.
- **Notfall- und Wiederherstellungsprozesse:** Abfrage der Notfallpläne und Datenwiederherstellung im Falle eines Angriffs.
- **Sicherheitslücken und unzureichende Schutzmaßnahmen:** Überprüfung von Schwachstellen, die potenziell ausgenutzt werden könnten.
- **Angriffs- und Bedrohungsszenarien:** Identifikation von Gefährdungen für die IT-Infrastruktur.

Warum eine Sicherheitsanalyse?

- **Proaktive Risikominderung:** Durch frühzeitige Identifikation von Schwachstellen können Sie potenzielle Angriffe verhindern, bevor sie zum Problem werden.
- **NIS2-Konformität:** Wir helfen Ihnen dabei, Ihre IT auf die gesetzlichen Anforderungen der NIS2-Richtlinie anzupassen.
- **Vermeidung von Strafen:** Apotheken müssen sicherstellen, dass ihre IT-Systeme ausreichend geschützt sind, um mögliche Strafen oder rechtliche Folgen zu vermeiden.



Verstöße gegen NIS2 sind kein Bagatelldelikt

Unternehmen wie z.B. Apotheken, die ihre Pflichten nach NIS2 nicht erfüllen – etwa indem sie Sicherheitsmaßnahmen vernachlässigen oder Meldefristen nicht einhalten – müssen mit spürbaren Konsequenzen rechnen.

Die nationalen Aufsichtsbehörden haben das Recht, Vor-Ort-Prüfungen durchzuführen, Dokumentationen einzufordern und bei Bedarf Bußgelder zu verhängen.

Und diese können empfindlich ausfallen: Je nach Unternehmensgröße und Branche drohen Strafen von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes – je nachdem, welcher Betrag höher ist.





Empfehlung

Um diese Risiken zu vermeiden, sollten Unternehmen:

- Eine umfassende IT-Sicherheitsanalyse durchführen
- Angemessene Sicherheitsmaßnahmen implementieren
- Mitarbeiterschulungen zur Sensibilisierung für Cybersicherheit anbieten
- Ein effektives Notfallmanagement etablieren

Die Einhaltung der NIS2-Richtlinie ist nicht nur gesetzliche Pflicht, sondern auch ein wichtiger Schritt zur Sicherung der Unternehmensintegrität und des Kundenvertrauens.

Vorteile für Ihre Apotheke

- Schutz vor Cyberangriffen und Datenverlust
- Erfüllung gesetzlicher NIS2-Anforderungen ohne großen Aufwand
- Vertrauensaufbau bei Kunden und Partnern durch hohe Sicherheitsstandards
- Individuelle Handlungsempfehlungen zur Verbesserung Ihrer IT-Sicherheit



Bleiben Sie informiert

Für aktuelle Hinweise und weiterführende Informationen empfehlen wir den Besuch der offiziellen Website des [Bundesamts für Sicherheit in der Informationstechnik \(BSI\)](#).

Dort können Sie auch eine [Betroffenheitsprüfung](#) durchführen, um zu prüfen, ob Ihr Unternehmen von aktuellen Sicherheitsrisiken oder gesetzlichen Vorgaben – etwa im Zusammenhang mit NIS2 – betroffen ist.



Nächste Schritte

Kontaktaufnahme

1. **Beratungsgespräch:** Wir beraten sie umfassend.
2. **Durchführung der Sicherheitsanalyse:** Wir prüfen Ihre IT-Infrastruktur und machen einen Sicherheitscheck. Speziell zugeschnitten auf die Anforderungen von Apotheken.
3. **Protokoll und Nachbesprechung:** Sie erhalten einen detaillierten Bericht mit klaren Handlungsempfehlungen.

Unsere Lösung



Beratungsgespräch



Sicherheitscheck



Protokoll
& Nachbesprechung

Kontaktieren Sie uns noch heute und sichern Sie sich Ihre Sicherheitsanalyse.

E-Mail: m.keimig@bitma.de | Telefon: [+49 9131 / 61 66 59 0](tel:+4991316166590)

IT ist unsere Bestimmung, Prozessoptimierung unsere Mission



1500 Kunden
deutschlandweit



28 Mitarbeiter



Über 20 Jahre Erfahrung



Kontakt

Head Office	+49 9131 616 659 0
Support	+49 9131 616 659 50
Mail	info@bitma.de
Web	www.bitma.de

BITMA

SOLUTIONS



Haben Sie ein spezielles Anliegen? Brauchen Sie eine individuelle Lösung? Ob grobe Idee oder konkrete Vorstellung — teilen Sie uns gern Ihre Wünsche mit. Wir nehmen alle Maße, bevor wir ein Produkt passgenau auf Ihr Unternehmen zuschneiden. Mit unserer Erfahrung haben Sie eine große Vielfalt an Möglichkeiten.

“Lassen Sie uns gemeinsam besprechen, wie wir auch Ihren Arbeitsalltag effizienter gestalten können. Getreu unserem Motto - **Platz schaffen, Ressourcen sparen, Zeit nutzen.**”

