ABDA

HINWEISE FÜR EIN IT-SICHERHEITSKONZEPT FÜR APOTHEKEN

Version	Datum	Kurzbeschreibung	Durchgeführt von
1.0	01.08.2025	Erstversion	ABDA

Disclaimer:

Dieses Dokument wurde sorgsam erarbeitet, um Ihnen in Verbindung mit der Musteranforderungsprüfliste einen ersten Überblick zum Thema IT-Sicherheit für Ihre Apotheke zu ermöglichen und Ihnen mögliche Lücken in der Absicherung aufzuzeigen. Eine vollständige Sicherheit kann weder allgemein noch im Apothekensektor erreicht werden. Vielmehr dient das vorliegende Dokument der Schaffung eines Bewusstseins für digitale Sicherheit in Apotheken und bietet Ihnen als Apotheker*in, insbesondere der Apothekenleitung wertvolle Hinweise zur Erstellung eines Sicherheitskonzeptes.

Dieses Dokument erhebt daher keinen Anspruch auf Vollständigkeit und betont ausdrücklich die Eigenverantwortung jeder Apotheke. IT-Sicherheit kann auf verschiedenen Wegen erreicht werden, daher besteht keine Verpflichtung, die hier vorgeschlagenen Maßnahmen umzusetzen. Die ABDA empfiehlt jedoch jeder Apothekenleitung, sich eingehend mit dem Thema auseinanderzusetzen. Dieses Dokument kann dabei als wertvoller Einstiegspunkt dienen.

Datenschutz und IT-Sicherheit sind zwar eng miteinander verbunden, stellen jedoch unterschiedliche Disziplinen dar. Während IT-Sicherheit den Schutz vor unbefugtem Zugriff auf Systeme und Daten sowie die Sicherstellung der Verfügbarkeit und Integrität der IT-Infrastruktur umfasst, konzentriert sich der Datenschutz auf den rechtlichen Umgang mit personenbezogenen Daten und deren Schutz gemäß den Vorgaben der Datenschutzgrundverordnung (DSGVO). Beide Bereiche sind gleichermaßen wichtig und sollten in Ihrer Apotheke jeweils gezielt adressiert werden, um einen umfassenden Schutz sowohl der digitalen Infrastruktur als auch der personenbezogenen Daten zu gewährleisten.

Bei konkreten Fragen zu Ihrer Apotheke kontaktieren Sie Ihren IT-Dienstleister. Bei Fragen zur Verwendung oder Weitergabe des Dokuments wenden Sie sich bitte an die ABDA – Bundesvereinigung Deutscher Apothekerverbände e.V.

INHALTSVERZEICHNIS

1. Vorbemerkung 3
2. Methodik/Vorgehen 6
3. Sicherheitsmanagement 7
3.1 Struktur des Sicherheitsmanagements 7
3.2 IT-Sicherheitsprozesse 7
3.3 IT-Sicherheitsrichtlinien 7
3.4 Sensibilisierung und Schulung 7
3.5 Incident Management 8
4. IT-Strukturanalyse 8
5. Schutzbedarfsfeststellung 10
5.1 Schutzziele 10
5.2 Vertraulichkeitsklassen 11
5.3 Schadensszenarien 12
5.3.1 Verstoß gegen Gesetze/Vorschriften/Verträge 12
5.3.2 Beeinträchtigung des informationellen Selbstbestimmungsrechts 12
5.3.3 Beeinträchtigung der persönlichen Unversehrtheit 13
5.3.4 Beeinträchtigung der Aufgabenerfüllung 14
5.3.5 Negative Innen- oder Außenwirkung 15
5.3.6 Finanzielle Auswirkungen 16
5.3.7 Kommunikationsverbindungen/Datenübertragungen mit Externen 17
5.4 Zusammenfassung der Ergebnisse der Schadensszenarien 18
6. Restrisiko 19
7. Umsetzungsplanung 20

1. Vorbemerkung

In der heutigen komplexen und dynamischen Welt steigen die Anforderungen an Sicherheit, insbesondere an Informationssicherheit und Datenschutz, kontinuierlich. Diese Entwicklung wird unter anderem auf Grund zunehmender globaler Konflikte verstärkt. Parallel dazu haben sich die Anforderungen an Unternehmen im Bereich der Kommunikation und digitalen Unterstützung von Geschäftsprozessen deutlich erhöht, was zu möglichen Schwachstellen im Bereich der Informationssicherheit führen kann, die teilweise verheerende Konsequenzen für die betroffenen Unternehmen haben können.

Auch Apotheken sind von diesen Veränderungen betroffen. Spätestens seit der Einführung der Telematikinfrastruktur sind Apotheken vor Ort hochdigitalisierte Einrichtungen, in denen zahlreiche geschäftskritische Prozesse digital ablaufen. Der Schutz dieser Prozesse und der dabei verarbeiteten Daten ist daher von zentraler Bedeutung.

Mit dem vorliegenden Dokument möchte die ABDA – Bundesvereinigung Deutscher Apothekerverbände e.V. den Apotheken ein praxistaugliches Werkzeug an die Hand geben, um in die Thematik der IT-Sicherheit unkompliziert einzusteigen und effizient bewerten und bei Bedarf zu verbessern. Dieses Dokument wurde unter Einbeziehung der Perspektiven verschiedener IT-Kompetenzzentren erstellt und überarbeitet, darunter der ADAS, das Bundesamt für Sicherheit in der Informationstechnik sowie ausgewählte Apothekerinnen und Apotheker.

Im Falle eines Unternehmens, das schlecht oder gar nicht vorbereitet Opfer eines Cyberangriffs wird, haftet die Geschäftsleitung und somit Sie als Apothekeninhaber*in. Einen Verzicht der Haftung schließt das Gesetz explizit aus – und macht IT-Sicherheit damit zur Chefsache. Um als Unternehmen einen wirksamen Schutz in allen relevanten Sicherheitsaspekten zu etablieren, ist die IT-Sicherheit verbunden mit konkreten technischen Maßnahmen nur ein kleiner Teil der gesamten Sicherheit der Organisation. Folgerichtig muss sich die IT-Sicherheit als Teil eines ganzheitlichen Sicherheitskonzeptes in die Organisation einfügen. Die Erstellung eines IT-Sicherheitskonzeptes kann hierbei als Startpunkt für die Erstellung eines übergreifendes Sicherheitskonzeptes dienen.

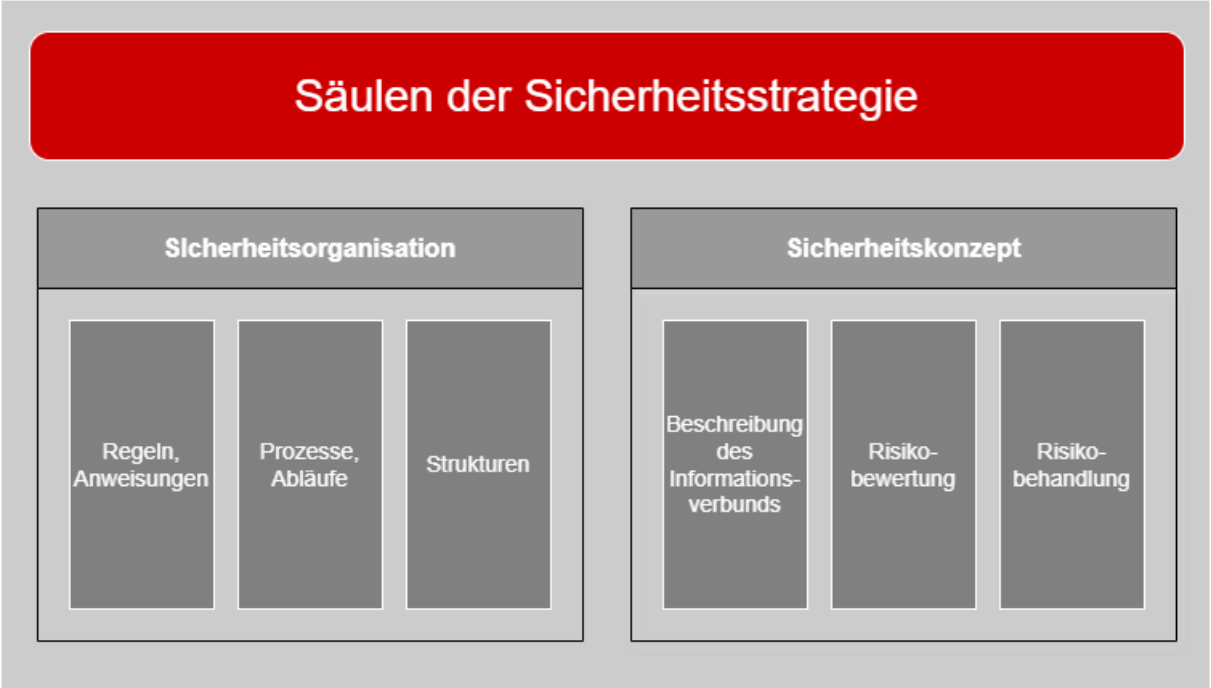

Abbildung 1 *Bausteine der Sicherheitsstrategie*

Die Abbildung veranschaulicht die wesentlichen Säulen einer umfassenden Sicherheitsstrategie, die auch für Apotheken von hoher Relevanz ist. Sie gliedert sich in zwei zentrale Bereiche:

1. Sicherheitsorganisation:

Eine strukturierte Sicherheitsorganisation ist essenziell, um Risiken im Apothekenbetrieb systematisch zu minimieren. Sie umfasst:

- **Regeln und Anweisungen**: Klare Vorgaben und Verhaltensrichtlinien, beispielsweise zur IT-Sicherheit, dem Umgang mit sensiblen Patientendaten oder der Zugriffskontrolle auf Arzneimittellager und Rezepturdokumentation.
- **Prozesse und Abläufe**: Standardisierte Verfahren, die eine sichere und effiziente Abwicklung von Arbeitsabläufen gewährleisten, etwa für die Medikamentenausgabe, das Bestandsmanagement oder die Validierung von Rezepten.
- **Strukturen**: Eine definierte Rollen- und Aufgabenverteilung, die sicherstellt, dass alle sicherheitsrelevanten Maßnahmen konsequent umgesetzt werden, sei es durch den Apothekenleiter, das pharmazeutische Personal oder die IT-Administration.

2. Sicherheitskonzept:

Ein wirksames Sicherheitskonzept schützt nicht nur Patientendaten, sondern trägt auch zur Integrität und Nachvollziehbarkeit pharmazeutischer Prozesse bei. Es umfasst:

- **Beschreibung des Informationsverbunds**: Eine detaillierte Erfassung aller sicherheitskritischen Systeme, darunter das Warenwirtschaftssystem, digitale Rezeptverwaltung und Datenbanken mit Kundenhistorien.
- **Risikobewertung**: Eine regelmäßige Analyse potenzieller Gefahren, beispielsweise durch Cyberangriffe, Datenschutzverstöße oder fehlerhafte Medikamentenlieferungen.
- **Risikobehandlung**: Die Implementierung geeigneter Schutzmaßnahmen, wie Zwei-Faktor-Authentifizierung für digitale Systeme, Zugriffsbeschränkungen oder Notfallpläne für IT-Ausfälle.

Oftmals werden Maßnahmen zur Stärkung der IT-Sicherheit wie die Erstellung eines IT-Sicherheitskonzeptes oder die Umsetzung dazugehöriger technischer und organisatorischer Maßnahmen als kostspielig, unpraktikabel oder unnötig bürokratisch empfunden. Dies entspricht in der Regel allerdings nicht der Realität, da es oftmals die einfachsten und günstigsten Maßnahmen sind, die den meisten Nutzen entfalten. Ein einfaches Beispiel hierfür wäre das Sperren von Arbeitsplatzrechnern, wenn man den Arbeitsplatz verlässt. Damit diese Maßnahmen allerdings ihre Wirkung voll entfalten können, ist eine fortlaufende Ausrichtung und Sensibilisierung aller Mitarbeitenden unerlässlich. Da die IT-Landschaft einer Apotheke sehr heterogen ist, ist es im Rahmen eines übergreifenden Dokumentes nicht möglich, jede Individualität abzudecken. Dies gilt insbesondere für Spezialfälle, welche normalerweise gar nicht oder nur sehr selten in einer Apotheke vorkommen. Daher sollte zu jedem Zeitpunkt kritisch hinterfragt werden, ob und zu welchem Grad dieses Dokument alle relevanten Systeme bzw. Maßnahmen berücksichtigt.

Hinweis für die Praxis:

Neben der IT-Sicherheitsprüfliste die Sie dabei unterstützt, schnell und effizient erste wichtige Maßnahmen umzusetzen und so ein hohes Maß an Sicherheit zu erreichen, können Sie für eine weitere Betrachtung des Themas bspw. die Bausteinen des IT-Grundschutzkompendiums nutzen sowie die verschiedenen BSI Grundschutz Standards.

2. METHODIK/VORGEHEN

Das vorliegende Dokument in seiner ersten Fassung orientiert sich an dem IT-Grundschutz des BSI, wurde jedoch bewusst vereinfacht, um einen praxisnahen Leitfaden für Apotheken zu erstellen. Ziel ist es, auch Apotheken mit begrenzten Ressourcen eine effektive Basisabsicherung der IT-Infrastruktur zu ermöglichen und dabei die spezifischen Anforderungen der Apothekenbranche zu berücksichtigen. Zu Beginn erfolgt eine IT-Strukturanalyse, bei der alle eingesetzten IT-Komponenten, Schnittstellen und Kommunikationswege erfasst werden. Dabei werden sowohl interne Zuständigkeiten als auch externe Verantwortlichkeiten, etwa durch Dienstleister, geklärt. Diese Analyse bildet die Grundlage für alle weiteren Schritte. Ein zentrales Element dieses Dokumentes ist die Festlegung des Schutzbedarfs nach dem Maximumprinzip. Der höchste Schutzbedarf eines Szenarios wird für die betroffenen Informationen, Anwendungen, Systeme, Netzverbindungen und Räume übernommen, unabhängig von geringeren Einstufungen in anderen Szenarien. Stellen wir uns beispielsweise die elektronische Patientenakte vor: Diese enthält sowohl allgemeine Kundendaten als auch besonders schützenswerte Gesundheitsdaten. Obwohl einige Daten (z.B. Name oder Adresse) einen geringeren Schutzbedarf haben könnten, wird der **höchste Schutzbedarf** aus dem Szenario der sensiblen Gesundheitsdaten übernommen.

Damit wird sichergestellt, dass kein wesentliches Risiko übersehen wird. Ziel ist es, ein ausgewogenes Verhältnis zwischen Sicherheitsniveau und Ressourceneffizienz zu erreichen. Auf Basis der Schutzbedarfsfeststellung werden mögliche Risiken abgeleitet, um besonders schützenswerte Systeme und Daten, wie Patientendaten oder abrechnungsrelevante Informationen, zu priorisieren. Mithilfe der beiliegenden Prüfliste können daraus die notwendigen Maßnahmen abgeleitet und deren aktueller Umsetzungsstand bewertet werden. Dazu gehören unter anderem regelmäßige Software-Updates. Ein weiterer wichtiger Aspekt ist die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter. Nur durch ein gut geschultes Team, das sicherheitskritische Situationen erkennt und angemessen handelt, können die getroffenen Maßnahmen ihre volle Wirkung entfalten. Zum Abschluss wird eine Umsetzungsplanung erstellt, der die Maßnahmen priorisiert und deren Implementierung vorbereitet. Hierbei ist ein realistischer Zeitplan ebenso entscheidend, wie die Berücksichtigung der verfügbaren Ressourcen. Die Wirksamkeit der Sicherheitsstrategie wird durch regelmäßige Überprüfungen und Anpassungen sichergestellt, um auf neue Bedrohungen und Entwicklungen flexibel reagieren zu können.

3. Sicherheitsmanagement

Das Sicherheitsmanagement spielt eine zentrale Rolle bei der Gewährleistung der IT-Sicherheit innerhalb einer Apotheke. Im Folgenden werden einige Grundelemente dargestellt, die im Rahmen des Sicherheitsmanagements berücksichtigt werden sollten. Das übergeordnete Ziel des Sicherheitsmanagements sollte es sein, einen hohen Grad an IT-Sicherheit zu gewährleisten und gleichzeitig die betrieblichen Prozesse der Apotheke zu unterstützen. Es ist wichtig zu verstehen, dass IT-Sicherheit ein fortlaufender Prozess ist und das Sicherheitsmanagement daher ständig verbessert und an neue Herausforderungen und Bedrohungen angepasst werden muss. Daher ist es auch essenziell, die Transparenz in der Apotheke zu erhöhen, um so potenzielle Sicherheitslücken zu schließen.

3.1 Struktur des Sicherheitsmanagements

Die Struktur des Sicherheitsmanagements sollte so organisiert sein, dass eindeutige Rollen und Verantwortlichkeiten festgelegt sind. Eine bestimmte Person in Ihrer Apotheke sollte die Hauptverantwortung für das IT-Sicherheitsmanagement tragen, die finale Verantwortung liegt jedoch immer bei der Geschäftsführung. Darüber hinaus sollten alle Mitarbeitenden in den Sicherheitsprozess einbezogen werden und einen aktiven Beitrag zur Sicherheit der von ihnen genutzten Systeme leisten.

3.2 IT-Sicherheitsprozesse

Die IT-Sicherheitsprozesse einer Apotheke sollten umfassend sein und eine regelmäßige Risikobewertung, die Implementierung und Überprüfung von Sicherheitsmaßnahmen sowie eine kontinuierliche Überwachung der IT-Systeme beinhalten. Zusätzlich sollte das IT-Sicherheitskonzept der Apotheke regelmäßig auf Aktualität überprüft und an neue Gegebenheiten angepasst werden.

3.3 IT-Sicherheitsrichtlinien

Die IT-Sicherheitsrichtlinien einer Apotheke sollten vielfältige Bereiche abdecken, einschließlich Zugangskontrolle, Datenschutz, Datensicherung und Benutzerverwaltung. Beispiele hierzu finden Sie in der Musterprüfliste. Diese Richtlinien sollten allen Mitarbeitenden bekannt sein und regelmäßig aktualisiert werden.

3.4 Sensibilisierung und Schulung

Die Sensibilisierung und Schulung der Mitarbeitenden im Bereich der IT-Sicherheit ist von entscheidender Bedeutung. Der alte Spruch „Eine Kette ist nur so stark wie das schwächste Glied“ gilt heute mehr als je zuvor. Regelmäßige Schulungen und

Informationsveranstaltungen sorgen dafür, dass im Team ein Bewusstsein für IT-Sicherheit geschaffen wird.

3.5 Incident Management

Wenn es in der Apotheke zu IT-Problemen kommt – z. B. durch einen Systemausfall oder einen Hackerangriff – muss schnell und gezielt gehandelt werden. Dafür sollte es einen klaren Ablaufplan geben:

- Wie wird ein Problem erkannt?
- Wer wird informiert?
- Was ist zu tun?

Wichtig ist, dass die Betriebsfähigkeit möglichst schnell wiederhergestellt werden kann. Zu den Kernelementen des Incident Managements gehören regelmäßige Datensicherungen, Ersatzlösungen für wichtige Geräte und ein Notfallplan für den Ernstfall.

4. IT-Strukturanalyse

Das Ziel der IT-Strukturanalyse ist es, einen Überblick über die wesentlichen IT-Komponenten der Apotheke vor Ort zu erhalten. Dabei beschränkt sich der Untersuchungsgegenstand auf die in der Offizin sowie im Backoffice betriebene IT-Komponenten. Die Telematikinfrastruktur (TI) wird hierbei außenvor gelassen, da die Sicherheit der TI von der gematik in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik verantwortet wird.

Folgend wird die interne IT-Landschaft mittels eines Diagramms bzw. tabellarisch dargestellt. Prüfen Sie kritisch, ob Ihre IT-Komponenten dort enthalten sind und tragen Sie diese ggf. nach Die folgende Tabelle kann genutzt werden, um die fachliche bzw. technische Zuständigkeit für die jeweiligen Komponenten einzutragen. Dies könnten bspw. IT-Dienstleister, Softwareunternehmen aber auch interne Mitarbeiter sein.

Komponente/n	Technische/fachliche Verantwortung
Arbeitsplatz-PC + Peripherie (Maus, Tastatur, etc.)	
Kassensystem + EC-Kartenterminal	
Warenwirtschaft (Wawi)	
Drucker	
Spezieller Rezeptdrucker	
Dokumenten/Rx-/Barcode-Scanner	
Router/Switch	
Tresor	
Festnetztelefon/Fax	
Bewegliche Datenträger (USB-Sticks, CDs, etc.)	
Zutrittssysteme	
Kommissionierer	
Mobile Endgeräte	
Cloud(-Dienste)	
Videoüberwachung	
Werbetafeln (digital)	
Sensoren, Alarmanlage	
Klimaanlage/Kühlung	

Tabelle 1 IT-Komponenten

5. SCHUTZBEDARFSFESTSTELLUNG

Die Schutzbedarfsfeststellung (SBF) hat zum Ziel zu ermitteln, welches Schutzniveau für Geschäftsprozesse sowie den dazugehörenden verarbeiteten Daten ausreichend bzw. angemessen ist. In der Methodik des IT-Grundschutzes, an dem sich in diesem Dokument orientiert wird, existieren drei Schutzbedarfsklassen (siehe Tabelle 2). Abweichend von der Grundschutzmethodik wird hier nicht jede Anwendung bzw. jeder Geschäftsprozess einzeln analysiert, sondern lediglich eine Betrachtung verschiedener Schadenszenarien und der betroffenen Schutzziele vorgenommen. Die hier betrachteten Szenarien wurden den BSI-Standards 100-2 und 200-2 entnommen. Zur Ermittlung der Risiken werden ggf. die Vertraulichkeitsklassen in die Betrachtung einbezogen.

Schutzbedarf	Schadenspotenzial
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar
„hoch“	Die Schadensauswirkungen können beträchtlich sein
„sehr hoch“	Die Schadensauswirkungen können ein existenzielles, bedrohliches, katastrophales Ausmaß erreichen

Tabelle 2 Schutzbedarfskategorien nach BSI-200-2

5.1 SCHUTZZIELE

Die **Schutzziele** werden aus der *ISO 27001* Norm entnommen. Diese Norm kennt die folgenden drei Schutzziele:

1. **Vertraulichkeit**
   Das Ziel der Vertraulichkeit besteht darin, Daten vor unbefugtem Zugriff zu schützen. Hierbei ist es unerheblich, ob dies aufgrund von datenschutzrechtlichen Erwägungen oder zum Schutz von Betriebsgeheimnissen, die dem Geschäftsgeheimnisgesetz unterliegen, geschieht. Eine exakte Abgrenzung der getroffenen Maßnahmen zu denen mit dem Schutzziel der Integrität ist hierbei nicht immer möglich oder sinnvoll.
2. **Integrität**
   Die Sicherstellung der Integrität von Informationen umfasst mehrere Aspekte. Dazu zählt der Schutz vor ungewollten oder nicht nachvollziehbaren Änderungen.

3. **Verfügbarkeit**
   Die Verfügbarkeit von Informationen bezieht die beteiligten Anwendungen bzw. Dienste in das Schutzziel ein. So kann der Ausfall einer Anwendung eine

erhebliche Auswirkung auf die Durchführbarkeit von Geschäftsprozessen haben. Der Zweck des Verfügbarkeitsziels besteht also darin, nicht akzeptable Verzögerungen im Abruf von Informationen oder Ausfälle der informationsverarbeitenden Systeme zu verhindern.

5.2 VERTRAULICHKEITSKLASSEN

Die Klassifizierung von Daten nach Vertraulichkeitsklassen dient dazu, Informationen oder Daten basierend auf ihrem Schutzbedarf hinsichtlich Vertraulichkeit systematisch zu kategorisieren. Diese Vorgehensweise wird in Organisationen häufig angewendet, um passende Sicherheitsmaßnahmen zu ergreifen, die den Anforderungen der unterschiedlichen Datenarten gerecht werden.

Hierzu wird in vier verschiedene Vertraulichkeitsklassen Unterschieden:

- **K1 - Öffentlich**
  Daten sind öffentlich zugänglich und können ohne Beschränkungen verbreitet werden. Sie enthalten in der Regel keine sensiblen oder vertraulichen Informationen, z.B. öffentliche Ankündigungen oder Aushänge.
- **K2 - Intern**
  Daten sind für interne Mitarbeiter*innen oder bestimmte Gruppen innerhalb der Apotheke bestimmt. Sie können betriebsinterne Informationen oder Projektdaten enthalten, die nicht für die Öffentlichkeit bestimmt sind. Der Zugriff auf diese Daten sollte beschränkt sein.
- **K3 - Vertraulich**
  Daten sind vertrauliche Informationen, die einen höheren Schutzbedarf haben, z.B. Kundendaten oder finanzielle Informationen. Der Zugriff sollte strenger kontrolliert werden und es müssen zusätzliche Sicherheitsmaßnahmen wie Verschlüsselung oder Zugriffskontrollen implementiert werden.
- **K4 - Streng vertraulich**
  Daten sind von höchster Vertraulichkeit und bergen das größte Risiko für die Apotheke. Hierzu gehören hochsensible Informationen wie medizinische Patientendaten, geistiges Eigentum oder rechtliche Dokumente. Der Zugriff auf K4-Daten sollte stark eingeschränkt werden und es sind strenge Sicherheitsprotokolle erforderlich, um deren Schutz zu gewährleisten.

Die Ergebnisse dieser Datenklassifizierung können direkt in die Bewertung möglicher Schadenszenarien einfließen und unterstützen die Identifikation geeigneter Schutzmaßnahmen.

5.3 SCHADENSSZENARIEN

Im folgenden Abschnitt wird die Gefährdungslage anhand verschiedener Szenarien eruiert. Hierbei wird für jedes Szenario eine Schutzniveau vorgeschlagen und begründet.

 Hinweis für die Praxis:

Für die Auswahl und Priorisierung von geeigneten Schutzmaßnahmen kann es hilfreich sein, die schützenswertesten Daten sowie die Systeme, in denen sie verarbeitet werden zu kennen. Insbesondere Daten der Kategorien K3 und K4 sind hierbei interessant.

5.3.1 Verstoß gegen Gesetze/Vorschriften/Verträge

Es kann zu erheblichen Folgen kommen, wenn die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten in Apotheken verletzt werden. Die Schwere des Schadens hängt oft davon ab, welche rechtlichen Konsequenzen daraus resultieren können. Die Anzahl an relevanten Vorschriften in der Apotheke sind sehr vielseitig und reichen vom Grundgesetz, über die DSGVO, der Apothekenbetriebsordnung bis zum Urheberrechtsgesetz (u.v.m.).

Folgende Fragen können unterstützend sein:

- In welchem Maße wird durch einen Verlust der Integrität und/oder Vertraulichkeit gegen Gesetze bzw. Vorschriften verstoßen?
- Gibt es vertragliche Bindungen für bestimmte einzuhaltende Termine?

Betrachtet man die vielfältigen Regularien, welche eine Apotheke erfüllen muss, scheint ein nicht unerheblicher Verstoß gegen Gesetze/Vorschriften/Verträge als durchaus wahrscheinlich, sollte es zu einem IT-Sicherheitsvorfall kommen. Weshalb wir hier regelmäßig ein sehr hohen Schutzbedarf für angemessen halten. Mehr dazu in den folgenden Szenarien.

5.3.2 Beeinträchtigung des informationellen Selbstbestimmungsrechts

Bei der Nutzung von IT-Systemen und Anwendungen besteht die Gefahr einer Verletzung des informellen Selbstbestimmungsrechts bis hin zu einem Missbrauch personenbezogener Daten.

Beispiele einer Verletzung des informellen Selbstbestimmungsrechts sind:

- Unzulässige Erhebung oder Weitergabe personenbezogener Daten ohne Rechtsgrundlage
- Unbefugte Kenntnisnahme bei der Datenverarbeitung/Übermittlung personenbezogener Daten
- Nutzung von personenbezogenen Daten zu einem nicht zulässigen Zweck
- Verfälschung von personenbezogenen Daten in IT-Systemen oder bei der Übertragung

Folgende Fragen können unterstützend sein:

- Welche Schäden können für den Betroffenen entstehen, wenn seine personenbezogenen Daten nicht vertraulich behandelt werden?
- Welche Schäden würden für Betroffene entstehen, wenn personenbezogene Daten unabsichtlich verfälscht oder absichtlich manipuliert werden?
- Können bei Ausfall der Anwendung oder bei einer Störung einer Datenübertragung personenbezogene Daten verloren gehen oder verfälscht werden, so dass Betroffene in ihrer gesellschaftlichen Stellung beeinträchtigt werden oder gar persönliche oder wirtschaftliche Nachteile zu befürchten haben?

In vielen IT-Sicherheitsvorfällen, wie etwa bei Datenlecks, erhalten Unbefugte Zugriff auf personenbezogene Daten. Wenn Angreifer in ein System eindringen und Daten erbeuten, besteht das Risiko, dass diese Daten in falsche Hände geraten und somit die informationelle Selbstbestimmung verletzt wird. Da es sich in der Apotheke oftmals um Gesundheitsdaten mit einer besonderen Sensibilität handelt, kann hier von einem sehr hohen Schutzbedarf ausgegangen werden.

5.3.3 Beeinträchtigung der persönlichen Unversehrtheit

Die Fehlfunktion von IT-Systemen oder Anwendungen kann unmittelbar die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Die Höhe des Schadens ist am direkten persönlichen Schaden zu messen. Beispiele für solche Anwendungen und IT-Systeme sind medizinische Überwachungsrechner oder medizinische Diagnosesysteme.

Folgende Fragen können unterstützend sein:

- Kann durch das Bekanntwerden von Daten eine Person physisch oder psychisch geschädigt werden?
- Können Menschen durch manipulierte Programmabläufe oder Daten gesundheitlich gefährdet werden?

- Bedroht der Ausfall der Anwendung oder des IT-Systems unmittelbar die persönliche Unversehrtheit von Personen?
- Bedroht der Ausfall von einzelnen Anwendungen oder des gesamten IT-Systems unmittelbar die persönliche Unversehrtheit von Personen?

Ein häufiges Risiko für die persönliche Unversehrtheit bei IT-Sicherheitsvorfällen ist die fehlerhafte Medikation aufgrund manipulierter Daten. Wenn Patientendaten verfälscht oder gelöscht werden, kann der Apotheker ein falsches Medikament abgeben, das entweder nicht den medizinischen Bedürfnissen entspricht oder schädliche Wechselwirkungen verursacht. Ein weiteres Risiko entsteht, wenn aufgrund von Systemausfällen Medikamente nicht korrekt dokumentiert oder Bestellungen nicht verarbeitet werden. Dies kann insbesondere bei chronischen Erkrankungen oder in der Intensivversorgung zu einer Verzögerung der Medikation und einer Verschlechterung des Gesundheitszustands führen. Entsprechend kann muss hier von einem sehr hohen Schutzbedarf ausgegangen werden.

5.3.4 Beeinträchtigung der Aufgabenerfüllung

Insbesondere der Verlust der Verfügbarkeit einer Anwendung oder der Integrität der Daten kann die Aufgabenerfüllung der Apotheke erheblich beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

Beispiele hierfür sind:

- Fristversäumnisse durch verzögerte Bearbeitung
- Verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen
- Falsche Medikamentenherstellung aufgrund falscher Daten
- Unzureichende Qualitätssicherung durch Ausfall eines Systems

Folgende Fragen können unterstützend sein:

- Entstehen erhebliche Schäden, wenn die Aufgaben trotz verfälschter Daten wahrgenommen werden? Wann werden unerlaubte Datenveränderungen spätestens erkannt?
- Sind von dem Ausfall einzelner Anwendungen andere Anwendungen betroffen?
- Welche Anwendung benötigen eine möglichst dauerhafte Verfügbarkeit?

Das Gesundheitsrecht verpflichtet Apotheken, ihre Dienstleistungen so zu erbringen, dass die Bevölkerung jederzeit und flächendeckend mit Arzneimitteln versorgt wird.

Dies ergibt sich sowohl aus dem ApoG als auch der ApoBetrO. Dies ist nicht nur eine logistische, sondern auch eine rechtliche Verantwortung, die im öffentlichen Interesse liegt. Der Zugang zu Arzneimitteln wird als grundlegendes Recht im Gesundheitssystem angesehen. Sowohl der **Verlust der Verfügbarkeit** als der **Integrität** können zu einer Beeinträchtigung der Aufgabenerfüllung führen. Dies ist sowohl wegen ökonomischen Konsequenzen für die Apotheke als auch aufgrund von rechtlichen Auflagen nicht tolerierbar ist und führt somit regelhaft zu einem Schutzbedarf von **sehr hoch**.

5.3.5 Negative Innen- oder Außenwirkung

Durch den Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit in einer Anwendung können verschiedenartige negative Innen- oder Außenwirkungen entstehen, wie zum Beispiel der Ansehensverlust der Apotheke, Einbußen in der Konkurrenzfähigkeit oder auch ein verlorenes Vertrauen in die Arbeitsqualität der Apotheke. Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlustes oder des Verbreitungsgrades der Innen- oder Außenwirkung.

Die Ursachen für solche Schäden können unterschiedlich sein:

- Handlungsunfähigkeit durch IT-Ausfall
- Fehlerhafte Veröffentlichungen durch manipulierte Daten
- Fehlbestellungen durch mangelhafte Lagerhaltungsprogramme
- Nichteinhaltung von Verschwiegenheitserklärungen
- Schuldzuweisungen an die falschen Personen
- Zuspielen vertraulicher Informationen an die Presse

Folgende Fragen können unterstützend sein:

- Welche Konsequenzen ergeben sich für die Apotheke durch die unerlaubte Veröffentlichung der für die Anwendung gespeicherten schutzbedürftigen Daten?
- Welche Schäden können sich durch die Verarbeitung, Verbreitung oder Übermittlung falscher oder unvollständiger Daten ergeben?
- Können verfälschte Daten zu einer verminderten Produktqualität und damit zu einem Ansehensverlust führen?
- Schränkt der Ausfall der Anwendung die IT-Dienste für Externe ein?
- Verhindert der Ausfall von Anwendungen das Erreichen von Geschäftszielen?
- Ab wann wird der Ausfall der Anwendung extern bemerkt?
- Wird die Verfälschung von Daten öffentlich bekannt?

Vertraulichkeit ist ein integraler Bestandteil des Berufs des Pharmazeuten. Dies findet sich nicht zuletzt auch in den Berufsordnungen der Länderkammer wieder, welche das Vertrauensverhältnis zum Patienten und die Schweigepflicht als Grundlage für die pharmazeutische Arbeit definieren. Entsprechend wurde die Schweigepflicht auch im Strafgesetzbuch festgehalten. Daraus lässt sich ein potenziell immenser Schaden für die Apotheke im Fall der Verletzung des Vertrauensverhältnisses ableiten und somit kann hier musterhaft ein sehr hoher Schutzbedarf angenommen werden.

5.3.6 Finanzielle Auswirkungen

Durch die Verletzung eines der drei Schutzziele durch einen IT-Sicherheitsvorfall, werden in der Regel nicht unerhebliche finanzielle Schäden verursacht. Diese können bspw. durch den Verlust der Vertraulichkeit von Patientendaten, die Veränderung dieser oder den Ausfall von Anwendungen entstehen.

Beispiele dafür sind:

- Unerlaubte Weitergabe von Daten
- Manipulation von Transaktionsdaten in einem Abrechnungssystem
- Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste
- Unerlaubte Einsichtnahme in Geschäftsgeheimnisse
- Zusammenbruch des digitalen Zahlungsverkehrs
- Diebstahl oder Zerstörung von Hardware

Die Höhe des Gesamtschadens setzt sich aus mehreren Faktoren zusammen. Hierzu zählen direkte Kosten für Systemwiederherstellung, beauftragte IT-Sicherheitsexperten, Geldstrafen als auch indirekt entstehenden Kosten, etwa durch Imageschäden, welche den zukünftigen finanziellen Erfolg beeinträchtigen können.

Folgende Fragen können unterstützend sein:

- Kann die Veröffentlichung vertraulicher Informationen Regressforderungen nach sich ziehen?
- Gibt es in der Anwendung Daten, aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann?
- Können durch verfälschte Bestelldaten finanzielle Schäden entstehen?
- Ergeben sich durch den Ausfall der Anwendungen finanzielle Verluste aufgrund von verzögerten Zahlungen bzw. Zinsverlusten?
- Wie hoch sind die Reparatur- oder Wiederherstellungskosten bei Ausfall, Defekt, Zerstörung oder Diebstahl des IT-Systems?

IT-Sicherheitsvorfälle sowie Datenschutzvorfälle können nicht selten sowohl hohe interne Kosten, bspw. durch Arbeitsausfälle, notwendige Neubeschaffungen als auch externe erzeugen (Strafen bei unzureichenden Absicherungen, Schadensersatzforderungen von Betroffenen). Die Höhe des entstandenen Schadens kann insbesondere durch die besondere Sensibilität der betroffenen Daten existenzbedrohende Ausmaße annehmen. Daher kann auch hier von einem sehr hohen Schutzbedarf ausgegangen werden.

5.3.7 Kommunikationsverbindungen/Datenübertragungen mit Externen

Ebenso sind Kommunikationsverbindungen/Datenübertragungen, die die Grenzen des Apotheken-Netzes überschreiten, grundsätzlich als „kritisch“ einzustufen. Dies ist auch beim Umgang mit mobilen Datenträgern und Geräten zu berücksichtigen. Hier haben Sie als einzelne Apotheke nur bedingt Steuerungsmöglichkeiten, da zu einer Kommunikation immer mehrere Parteien gehören. Wenn Ihre Kommunikationspartner bspw. keinen verschlüsselten Mailverkehr unterstützen, können Sie nur bedingt darauf Einfluss nehmen. Besonders wichtig ist es daher, die Schwachstellen in Ihrer Kommunikation zu kennen und, wo möglich, auf sichere Datenübertragungswege zu wechseln.

5.4 Zusammenfassung der Ergebnisse der Schadensszenarien

Da in Apotheken sehr sensible Gesundheitsdaten verarbeitet werden, kann bei einem IT-Sicherheitsvorfall das Risiko einer Datenpanne oder eines Missbrauchs groß sein. Gesundheitsdaten gehören zu den am stärksten zu schützenden Daten und erfordern daher besondere Sorgfalt. Auch zeigen die vielfältigen Vorschriften, denen Apotheken unterliegen, dass bei einem IT-Sicherheitsvorfall ein erheblicher Verstoß gegen zahlreiche Auflagen und Verträge, sowie gravierende finanzielle Folgen zu erwarten sind. Diese Erkenntnis findet sich auch in der Betrachtung der Schadensszenarien wieder. Dies führt dazu, dass **Apotheken in der Regel einen sehr hohen Schutzbedarf haben**, um sowohl rechtliche, gesundheitliche als auch finanzielle Risiken zu minimieren. Sollten Sie in Ihrer persönlichen Bewertung zu einem abweichenden Ergebnis kommen, wäre eine kurze Erläuterung sinnvoll.

Gesamt ☐ normal ☐ hoch ☐ sehr hoch

Erläuterung zu abweichendem Schutzbedarf:

6. RESTRISIKO

In der IT-Sicherheit bezeichnet das Restrisiko die verbleibende Gefahr eines Sicherheitsvorfalls, nachdem alle angemessenen Schutzmaßnahmen implementiert wurden. Das bewusste Akzeptieren dieses Restrisikos ist essenziell für ein effektives Risikomanagement. Das Restrisiko entsteht durch verschiedene Faktoren, die sowohl technischer als auch organisatorischer Natur sein können. Beispielsweise durch unbekannte Schwachstellen, die ausgenutzt werden können, bevor ein Update verfügbar ist oder aber auch menschliches Versagen wie Fehlkonfigurationen, mangelndes Sicherheitsbewusstsein oder unvorsichtiger Umgang mit sicherheitskritischen Daten.

Zudem besteht moderne IT-Infrastruktur aus zahlreichen miteinander vernetzten Komponenten, wodurch potenzielle Angriffspunkte entstehen. Ein nahezu absolutes Sicherheitsniveau ist wirtschaftlich kaum bis gar nicht realisierbar, da Apotheken, wie alle kaufmännischen Unternehmungen stets zwischen Kosten, Effizienz und Sicherheit abwägen müssen. Hinzu kommt, dass sich die Bedrohungslandschaft kontinuierlich weiterentwickelt, sodass bestehende Schutzmaßnahmen umgangen werden können.

Obwohl das Restrisiko nie vollständig eliminiert werden kann, existieren verschiedene Strategien, um es auf ein akzeptables Maß zu reduzieren: Ein risikobasierter Sicherheitsansatz bedeutet, dass sich die Sicherheitsmaßnahmen an der Kritikalität der verarbeiteten Daten orientieren. Gezielte Backup- und Wiederherstellung-Strategien reduzieren das Schadenspotenzial im Falle eines erfolgreichen Angriffs. Da der Mensch oft die schwächste Sicherheitskomponente darstellt, sind regelmäßige Sensibilisierungen aller Mitarbeiter essenziell, um Sicherheitsbewusstsein und sichere Verhaltensweisen zu fördern.

Das Restrisiko ist eine unvermeidbare Realität in der IT-Sicherheit und sollte unbedingt als fester Bestandteil eines umfassenden Sicherheitskonzepts betrachtet werden. Durch ein kontinuierliches Sicherheitsmanagement, eine anpassungsfähige Sicherheitsstrategie und die Einbindung aller Beteiligten kann das Restrisiko auf ein akzeptables Maß reduziert werden.

 Hinweis für die Praxis:

Nutzen Sie die Musterprüfliste als Einstiegspunkt für Ihre Restrisikobetrachtung: Wo fehlen Ihnen Maßnahmen oder was war Ihnen ggf. bisher nicht bewusst? Welche Folgen könnten für Ihre Apotheke entstehen?

7. UMSETZUNGSPLANUNG

So planen Sie die Umsetzung:

1. **Maßnahmen nach Dringlichkeit sortieren:**
    - **P1 – Hohe Priorität:**
      Diese Maßnahmen sollten **sofort** umgesetzt werden, z. B. wenn sensible Patientendaten ungeschützt sind oder keine regelmäßigen Backups gemacht werden.
    - **P2 – Mittlere Priorität:**
      Diese Punkte sind wichtig, können aber innerhalb der nächsten Wochen oder Monate erledigt werden, z. B. Software-Updates einführen oder Mitarbeiterschulungen organisieren.
    - **P3 – Niedrige Priorität:**
      Diese Maßnahmen sind sinnvoll, aber nicht dringend, z. B. Einführung eines IT-Dokumentationssystems oder Optimierung vorhandener Prozesse.

 Hinweis für die Praxis:

Nutzen Sie die beigefügte IT-Sicherheitsprüfliste als Grundlage. Welche Maßnahmen sind bei Ihnen bereits erfüllt? Welche noch offen?

So behalten Sie den Überblick, können Risiken gezielt reduzieren und sorgen für eine sichere IT-Umgebung in Ihrer Apotheke.

2. **Zeitplan festlegen:**
   Notieren Sie zu jeder Maßnahme ein realistisches Ziel-Datum – also bis wann die Umsetzung erfolgen soll. Stimmen Sie das am besten mit Ihrem IT-Dienstleister ab.
3. **Zuständigkeiten klären:**
   Legen Sie fest, ob ein Mitarbeiter oder ein externer Dienstleister verantwortlich ist.
4. **Umsetzung regelmäßig überprüfen:**
   Planen Sie einen festen Termin (z. B. halbjährlich oder jährlich), um zu kontrollieren, ob alle Maßnahmen umgesetzt wurden oder ob neue Themen hinzugekommen sind.

GLOSSAR

Nr.	Begriff	Erläuterung
1	Incident	Ein Incident bezeichnet ein Ereignis, das den normalen Betrieb eines IT-Systems beeinträchtigt oder unterbricht. Dazu zählen Sicherheitsvorfälle, Fehler oder Störungen, die eine sofortige Behebung erfordern, um Schäden zu minimieren.
2	Incident Management	Incident Management ist der strukturierte Prozess zur Erkennung, Analyse und Behebung von Incidents in IT-Systemen. Ziel ist es, Störungen schnell zu beheben und den normalen Betriebsablauf wiederherzustellen.
3	BSI-Grundschutz	Der BSI-Grundschutz ist ein Konzept des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur systematischen Absicherung von IT-Systemen. Es bietet standardisierte Maßnahmen und Empfehlungen zur Verbesserung der Informationssicherheit in Organisationen.
4	Kontinuitätsmanagement	Kontinuitätsmanagement (Business Continuity Management) umfasst Strategien und Maßnahmen, um den Geschäftsbetrieb auch in Krisensituationen aufrechtzuerhalten. Ziel ist es, Ausfälle zu minimieren und wichtige Prozesse schnell wiederherzustellen.
5	Kryptographie	Kryptographie bezeichnet Prozesse der Verschlüsselung von Daten. Sie schützt Informationen vor unbefugtem Zugriff und Manipulation, indem sie Daten in eine unlesbare Form umwandelt, die nur durch autorisierte Personen entschlüsselt werden kann.
6	Informationelle Selbstbestimmung	Das Recht auf informationelle Selbstbestimmung bezeichnet die Freiheit jedes Einzelnen, über die Erhebung, Speicherung und Nutzung seiner persönlichen Daten zu entscheiden. Es ist ein Grundrecht und schützt die Privatsphäre im digitalen Zeitalter.
7	Cloud(-Dienst)	Begriffsbestimmung lt. §384 Nr. 5 SGB V: „Cloud-Computing-Dienst [ist] einen digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam genutzter Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind.“