MORGENSTERN

# Whitepaper

## Datenschutz & IT-Sicherheit im Healthcare-Sektor

morgenstern-privacy.com

MORGENSTERN

Dieses Whitepaper gibt dir einen grundsätzlichen Überblick über die gesetzlichen und praktischen Herausforderungen im Datenschutz und der IT-Sicherheit, denen sich Organisationen im Gesundheitswesen angesichts neuer Potenziale der Digitalisierung und zunehmender Cyber-Risiken stellen müssen.

**Brauchst du Rat?** Kontaktiere uns! Wir bei MORGENSTERN haben ein erfahrenes und hochspezialisiertes Team bestehend aus Anwälten, Datenschutz- und IT-Sicherheitsexperten!

contact@morgenstern-privacy.com

Große Himmelsgasse 1
D-67346 Speyer

Brauchst du Support und rechtliche Beratung bei Projekten basierend auf dem Krankenhaus-Zukunftsgesetz (KHZG)? Wir haben die notwenige Berechtigung auf Grundlage von § 21 Abs. 5 S. 1 KHSFV.

**Hier** geht's direkt zur Leistungsübersicht.

# I. Worum geht es?

Im Umgang mit Patientendaten kommen immer wieder Fragen zum Datenschutz und zur Informationssicherheit („IT-Sicherheit") auf. Diese Fragen beschäftigen angesichts zunehmender Digitalisierung und Automatisierung der Behandlungs- und Verwaltungsabläufe nicht nur die Akteure an „vorderster Front", insbesondere Organisationen und Träger wie Krankenhäuser, Praxen und Pflegedienste, sondern auch den Dienstleistungsbereich, sprich Anbieter im Bereich IT-, Telematikinfrastruktur und Sicherheitstechnologie sowie die wissenschaftliche und private Forschung.

## Chancen und Potenziale

Die Herausforderung für die oben genannten Stakeholder besteht letztlich darin, Innovation und moderne Technologien in deiner Organisation betreiben zu können und dabei rechtlich und operativ auf der sicheren Seite zu sein – aber was bedeutet das eigentlich?

Moderne Technologien erlauben dem Gesundheitssektor, Verfahren und Systeme bei der Behandlung von Patienten zu nutzen, die eine genauere Diagnostik, verbesserte Behandlungen und effizientere Prozesse ermöglichen. Die Integrationstiefe reicht von der digitalisierten Patientenverwaltung mittels Patienten- und Krankenhausinformations- und Verwaltungssystemen, der Implementierung von Telematikinfrastrukturen (E-Health), der virtuellen medizinischen

Patientenbetreuung bis hin zu automatisierten Warenwirtschaftssystemen und intelligenten Datenanalysen sowie Big-Data-Nutzungen.

## Herausforderungen und Bedrohungslagen

Die oben genannten Technologien sind für die Weiterentwicklung ärztlicher und pflegerischer Tätigkeiten elementar wichtig. Diese Technologien sind bzw. werden aber in komplexe regulatorische Rahmen eingebettet, die von Organisationen, die ihre Prozesse zukunftsfähig ausgestalten wollen, eingehalten werden müssen. Dabei entstehen gerade in Zeiten des Kostendrucks, der auf dem Gesundheitssektor lastet, erhebliche Zielkonflikte: Innovation vs. Rechtsbefolgung, KI-basierte Forschung vs. Datenschutz und Ethik, etc.

Die Digitalisierung birgt also nicht nur Chancen, sondern stellt für Organisationen aller Größen und Organisationsformen aufgrund der genannten Zielkonflikte auch Umsetzungshürden auf.

Am Horizont von Innovation und Digitalisierung tun sich für den Healthcare-Bereich – abseits aller Vorteile und Zielkonflikte – zudem einige dunkle Wolken auf:

Cyber-Angriffe und -vorfälle im Gesundheitsbereich nehmen weltweit zu. Im Jahr 2021 verursachten allein Datenlecks im Gesundheitsbereich Kosten in Höhe von 7,1 Mio. USD[1]. Weltweit sollen 74 % aller Gesundheitsorganisationen von Datenlecks betroffen gewesen sein. Mit der zunehmenden Digitalisierung und Vernetzung von Gesundheitssystemen aller Art gehen letztlich zunehmende digitale Risiken einher. Doch weshalb sind Einrichtungen des Gesundheitswesens, insbesondere Krankenhäuser, derart anfällig für solche Risiken?

[1] Bolkart, Statistiken zu Healthcare und Cyber-Security, Statista, 25.01.2022 (abrufen zuletzt am 20.02.2022)

- **Digitale Risikoursachen**

  Wohl die erheblichsten Risiken für Cybersicherheitsvorfälle aufgrund von Anwendungsfehlern und Cyberkriminellen gehen auf das Konto der eigenen IT-Systeme. Dort, wo interne Verwaltungssysteme, z.B. über die Cloud, betrieben werden, besteht immer das Risiko, dass Kriminelle auf diese Systeme zugreifen. Fehlende Awareness des Personals im Umgang mit Systemen und Daten kann zu Anwendungsfehlern, Datenlecks und Datenverlusten führen.

- **Risikofaktor Datenbedarf**

  Organisationen im Gesundheitswesen müssen Daten ihrer Patienten und anderer Betroffener verarbeiten, und zwar in einem erheblichen Umfang und in den meisten Fällen zumindest teildigitalisiert. Hinzu kommt, dass diese Daten, die Dokumentation und Akten über sehr lange Zeiträume (hier sprechen wir in der Regel von mindestens zehn Jahren) aufzubewahren sind. Wird schon allein ein Datensatz kompromittiert, sind die Folgen oft erheblich – letztlich sind darin extrem sensible Informationen enthalten. Den Betroffenen fehlen zudem eigene Interventionsmöglichkeiten, da sie keinerlei Einfluss darauf haben, wie und wo ihre Daten gehalten oder archiviert werden.

- **Der „The Winner-takes-it-all“-Effekt**
  Gelingt es Angreifern mit Schädigungsabsicht, sich Zugriff auf die IT-Systeme oder Daten zu verschaffen, sind diese häufig aufgrund fehlender Binnensegmentierung bzw. Trennung alle auf „einen Schlag“ zugänglich. Kommt es zum Einsatz von Verschlüsselungstrojanern auf betriebskritischen Systemen, haben Organisationen oftmals überhaupt keine andere Möglichkeit mehr, als die geforderten Erpressungsgelder klaglos zu zahlen, um die Systeme wieder in Betrieb nehmen zu können.

- **Fehlende Awareness der Leitungsebenen**
  Nach wie vor ist die notwendige Sensibilität für IT-Risiken und Datenschutz nicht wirklich in Leistungs- und Vorstandsebenen angekommen. Das ist gerade angesichts der momentanen Belastungssituation, die auf dem Gesundheitssektor liegt, vollkommen nachvollziehbar – kann aber bei Vorfällen, Prüfungen, für den Abruf von Fördermitteln und Geldern sowie bei der Versicherbarkeit von Cyberrisiken gravierende Folgen haben. Erschwerend kommt hinzu, dass die interne IT auch in größeren Einrichtungen häufig personell sehr dünn besetzt ist, was Folgeprobleme aufwirft: Es fehlt an internem Know-how und Kompetenzen über IT-, Daten- und Informationssicherheit.

- **Blackbox-IT und fehlende Updates**
  In der Praxis ein recht häufig vorkommender Fall. Eine Einrichtung hat zu einem bestimmten Zeitpunkt ein Digitalisierungsprojekt mit einem Dienstleister durchgeführt, der die neuen Systeme weiterhin betreut, hostet und pflegt. Alles kein Problem – so lange alles gut geht. Viele Organisationen – nicht nur im Gesundheitsbereich – stellen zu spät fest, wie abhängig sie von IT-Dienstleistern sind. Diese Abhängigkeit bringt Folgerisiken mit sich, die die Organisation auf Dauer nicht mehr beherrschen kann.

Doch wie lässt sich Innovation im Gesundheitswesen rechtssicher, gleichzeitig aber auch praktikabel und zukunftssicher umsetzen? Wie verhalten sich die geltenden rechtlichen Rahmenbedingungen zu den wesentlichen Digitalisierungsfragen dieser Branche und welche Fallstricke sind zu beachten?

Diesen Fragen und den wichtigsten Zusammenhängen gehen wir in diesem Whitepaper auf den Grund.

# II. Grundannahmen

Personenbezogene Daten, die im Gesundheitswesen anfallen, haben in der Regel einen sehr hohen Schutzbedarf. Dem risikobasierten Ansatz des Datenschutzrechts folgend, sind daher für diese Daten intensivere Schutzmaßnahmen zu ergreifen, als für Daten, die grundsätzlich keinen sehr hohen Schutzbedarf haben (wie z.B. Namen, Kontaktinformationen).

## 1. Der gesetzliche Rahmen für Datensicherheit und Datenschutz

Für Organisationen im Gesundheitswesen gelten vielfältige gesetzliche Rahmenbedingungen. Je nachdem, ob es sich um eine privat-, öffentlich- oder kirchenrechtliche Einrichtung handelt, sind für die jeweilige Organisation folgende Gesetze zum Datenschutz relevant:

1. Datenschutz-Grundverordnung (DS-GVO)
2. Bundesdatenschutzgesetz (BDSG)
3. Kirchliche Datenschutzgesetze
4. Landesdatenschutzrecht
5. Patientendatenschutzgesetz (PDSG)
6. B3S – Krankenhaus
7. BSI-Gesetz und KRITIS-Verordnung

Hinzu kommt eine Vielzahl besonderen berufs-, vorgangs- und einrichtungsbezogenen Vorschriften, die spezifische Vorgaben zur Nutzung, Ablage oder Weitergabe von medizinischen Daten haben:

1. Berufsordnungen Ärzte
2. Transfusionsgesetz
3. Transplantationsgesetz
4. Gendiagnostikgesetz
5. Infektionsschutzgesetz
6. Arzneimittelgesetz
7. Medizinproduktegesetz / Medizinproduktebetreiberverordnung
8. Strahlenschutzverordnung
9. Landeskrankenhausgesetze
10. Bestattungsgesetze des Bundes und der Länder
11. Bundesmeldegesetz
12. Personenstandsgesetz
13. Bundesmantelvertrag Ärzte (neu!)
14. Sozialgesetzbücher
15. Krebsregistergesetze

**Gesundheitsdaten**

1. Genetische Daten
2. Daten zum Sexualleben oder der sexuellen Orientierung
3. Teilweise Daten zu religiöser oder weltanschaulicher Überzeugung

*Das alles sind Datenarten, die in den einschlägigen Datenschutzgesetzen als besondere Datenkategorien bezeichnet und definiert werden. Die Besonderheiten ergeben sich im Schwerpunkt aus den besonderen Pflichten, die Organisationen im Umgang mit diesen Datenarten befolgen müssen.*

*Der hohe Schutzbedarf für diese Daten resultiert aus den typischen Risiken, denen diese Daten in bestimmten Fällen unterliegen können. Diese ergeben sich zunächst aus den drohenden Folgen möglicher Datenschutzverletzungen. Diese sind im Fall sensibler Daten wie Patientendaten aus Sicht der betroffenen Personen gravierender als im Fall von Daten, die nicht als besondere Datenkategorien gelten.*

Doch welche Risiken stehen konkret im Raum und anhand welcher tatsächlicher Szenarien sollten Organisationen ihre Maßnahmen ausrichten?

## 2. Datensicherheit im Datenschutz – Die Schnittstelle zur IT-Sicherheit

Welche Maßnahmen zum Schutz von Daten im Gesundheitswesen zu ergreifen sind, ist in den einschlägigen Gesetzen eher abstrakt bzw. nur zum Teil geregelt. Daher obliegt es in erster Linie den Organisationen im Gesundheitswesen, die in großem Umfang besondere Datenkategorien verarbeiten müssen, geeignete und angemessene Schutzmaßnahmen zu ergreifen.

Grundsätzlich sehen die Gesetze folgende Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus vor:

1. Pseudonymisierung, Anonymisierung und Verschlüsselung
2. Maßnahmen zur dauerhaften Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste
3. Maßnahmen zur raschen Widerherstellung der Verfügbarkeit der personenbezogenen Daten bei einem physischen oder technischen Zwischenfall
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Diese Maßnahmen sind stets am aktuellen Stand der Technik auszurichten. Organisationen im Gesundheitswesen sind daher gut beraten, die bestehenden Maßnahmen laufend auf dem neuesten Stand zu halten. Die verarbeitende Organisation ist hinsichtlich des Ergreifens und in Bezug auf die Angemessenheit des durch die Maßnahmen eingerichteten Datenschutzniveaus nachweisbelastet. Die Maßnahmen müssen also dokumentiert und fortlaufend kontrolliert werden.

Es ist außerdem zu beachten, dass die datenschutzrechtlichen Vorgaben tatsächlich nur auf die Verarbeitung von Daten mit Personenbezug anzuwenden sind. Regelungen, die sich auf die Sicherheit der IT-Anlagen und IT-Systeme der Organisationen beziehen, sind in den einschlägigen Datenschutzgesetzen nicht vorgesehen. Angesichts zunehmender Risiken für die IT-Strukturen von Organisationen im Gesundheitswesen dürfte eine Sicherheitsarchitektur, die nur auf der Grundlage der Datenschutzgesetze basiert, nicht ausreichend sein.

Gerade für den Krankenhausbereich und das Gesundheitswesen hat aber der Gesetzgeber hilfreiche Anforderungen an die IT-Sicherheit erarbeitet, die eine ganzheitliche Optimierung des Schutzes personenbezogener Daten und der dahinterstehenden IT-Systeme erlauben.

## 3. IT-Sicherheitsrechtliche Anforderungen

### Bedrohungslage und spezifische Schwachstellen

Der deutsche Gesetzgeber hat für Einrichtungen mit bestimmten Schwellwerten im Bereich Krankenhaus einen branchenspezifischen Sicherheitsstandard erarbeitet. Durch die ENISA (EU-Agency for Cybersecurity) wurden die Kernbedrohungen für Cyberrisiken in einem Report wie folgt genannt:

- **Malware, Viren, Ransomware**
  Hierbei handelt es sich um ganz klassische Schadprogramme und Verschlüsselungsangriffe, die häufig aufgrund menschlichen Verhaltens in den Systemen Schaden anrichten können.

- **BYOD**
  Risiken, die sich aus der Nutzung von Privatgeräten durch Personal ergeben, sind für Einrichtungen extrem schwer zu beherrschen, da nicht ohne Weiteres (z.B. durch ein MDM) zentrale Verwaltungs- und Sicherungsmaßnahmen auf diesen Geräten installiert werden können. Etwaige vorhandene technische Sicherheitsrichtlinien können daher nicht greifen bzw. laufen ins Leere.

- **Hijacking durch Crypto- und Medijacking**
  Dabei nutzen sogenannte Miner die Server- und Rechenleistung der Organisation, um Cryptowährung zu schürfen (sogenanntes Mining). Der Zugriff ist für die Organisation extrem schwer zu erkennen, da er meistens über die Netzwerke von Medizingeräten erfolgt, die in das Netzwerk eingebunden sind, aber veraltete Software haben, die ein Erkennen der Zugriffe meist nicht mehr zulässt.[2]

- **Social Engineering, Phishing und Cloning**
  Hierbei werden durch Betrug oder Manipulation Systeme, Anwendungen (z.B. der betriebliche E-Mail-Account oder sogar Geräte) von Kriminellen imitiert, um sich unerkannt Zugang zu Systemen zu verschaffen.

[2] Dabei handelt es sich meistens um Geräte, die nach dem Medizinproduktegesetz zertifiziert sind, da die darauf installierte Software nach Zertifizierung nicht mehr geupdated werden kann.

- **Medical Device Tampering**
  Dabei werden medizinische Geräte manipuliert, wodurch Daten, die die Geräte gewinnen, an Unbefugte fließen können oder sogar so manipuliert werden, dass sie von Angreifern ferngesteuert werden können.

- **Insider Treats**
  Wie der Name bereits befürchten lässt, handelt es sich bei Insider Threats um Bedrohungen von Innentätern. Diese können zwar auch auf einer Schädigungsabsicht (und damit auf einer in der Regel strafbaren Handlung) beruhen, oftmals liegen darin aber eher Risiken und Bedrohungen, die auf menschlichem und unabsichtlichem Fehlverhalten des Personals beruhen.

- **Denial of service**
  Häufig finden Denial-of-Service-(DOS)Angriffe auf Systeme und medizinische Dienste statt, die über das Internet oder Clouddienste bereitgestellt werden. Bei einem DOS-Angriff ist der Dienst nicht mehr verfügbar und kann nicht mehr genutzt werden.

## Informationsverbünde als Schutzobjekt und Angriffsziel

Zunächst ist festzuhalten, dass der Begriff IT-Sicherheit für die Abbildung der relevanten Prozesse, die rechtlich und operativ abgesichert werden müssen, viel zu kurz gegriffen ist. Korrekt wäre eigentlich der Begriff der Informationssicherheit. Informationssicherheit nimmt neben den IT-Systemen und Strukturen auch sämtliche Prozesse und Akteure in den Blick, vermittels derer in der Organisation (also der Praxis, dem MVZ, dem Krankenhaus, der Pflegeeinrichtung und im Rahmen outgesourcter Prozesse) Informationen verarbeitet werden.

## Schutzziele

Im Bereich des Gesundheitswesens sind grundsätzlich vier Schutzziele der Informationssicherheit durch die jeweiligen Betreiber zu gewährleisten:

- **Vertraulichkeit**
  Das Schutzziel Vertraulichkeit soll den Schutz von Informationen sicherstellen, die vor dem unbefugten bzw. unberechtigten Zugang geschützt sind.

- **Integrität**
  Integrität bezieht sich sowohl auf die Funktionalität und Unversehrtheit der Systeme, als auch auf die Unversehrtheit der relevanten Informationen.

- **Verfügbarkeit**
  Die Verfügbarkeit des Informationssystems ist dann gewährleistet, wenn es zu den vorgesehenen Zeiträumen (im Krankenhaus, also durchgehend, anderenfalls z.B. während der Geschäftszeiten) von allen Berechtigten und daran angeschlossenen Akteuren genutzt werden kann.

- **Authentizität**
  Authentizität ist dann gewährleistet, wenn und soweit alle Informationen und Zugriffe innerhalb des Informationsverbundes auf eine glaubwürdige („authentische“ Quelle) zurückzuführen sind. Das gilt sowohl für Berechtigungen auf der Nutzerebene, als auch auf der Ebene von Systemzugriffen, z.B. über Schnittstellen von Software, die auf Datenbanken (z.B. ein Praxisverwaltungssystem oder ein Abrechnungssystem) zugreifen können.

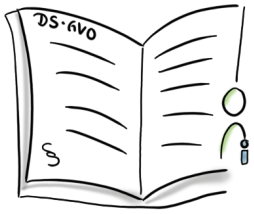
## III. Haftungsrisiken

Von der Management-Perspektive aus gesehen, also auf der Ebene der Geschäfts- und Einrichtungsleitungen, sind in Bezug auf die Einhaltung der Vorgaben von IT-Sicherheit und Datenschutz schon auf der zivilrechtlichen Ebene Haftungsrisiken relevant.

Vorstände und Geschäftsleitungen haben am Stand der Technik orientierte Maßnahmen zu ergreifen, die geeignet sind, den hohen Schutzbedarf der sensiblen personenbezogenen Daten und die Schutzziele der Informationssicherheit zu gewährleisten.

Diese Maßnahmen sind im Rahmen der IT- und Datenschutzcompliance regelmäßig auf ihre Wirksamkeit hin zu kontrollieren. Die Kontrollmaßnahmen sind zu dokumentieren. Speziell für Betreiber, die unter B3S fallen, muss die Wirksamkeit der Schutzmaßnahmen durch Zertifizierungen und Audits alle zwei Jahre nachgewiesen werden. Kann eine Organisation im Zuge eines Datenschutz- oder Informationssicherheitsvorfalls nicht nachweisen, ihren Prüf- und Kontrollpflichten nachgekommen zu sein, kann es sogar zum Haftungsdurchgriff auf die Mitglieder der jeweiligen Leitungsebene kommen.

Daneben stehen stets die spezialgesetzlichen Schadenersatz- und Bußgeldandrohungen (wie z.B. nach der DS-GVO).



MORGENSTERN

## IV. Lösungsansätze

### IT-Outsourcing nicht aus dem Blick verlieren! Verträge aufgeklärt abschließen!

Was im Rahmen dieses Whitepaper keinesfalls zu kurz kommen darf, ist die Steuerung und Prüfung von IT-Outsourcing. Das betrifft zum einen die Nutzung cloudbasierter Dienste im Gesundheitswesen. Die Einrichtung hat bereits bei der Einführung von Clouddiensten lückenlos zu dokumentieren, welche Informationen und Systeme überhaupt in der Cloud abgelegt bzw. aus der Cloud heraus betrieben werden dürfen. Im operativen Betrieb sind insbesondere verschlüsselte Datenablagen und verschlüsselte Datenübertragung in den Fokus zu nehmen.

Die Einbindung externer Dienste und Anbieter unabhängig davon, ob es sich um einen Clouddienst handelt oder nicht, ist aus dem modernen Klinik- und Praxisbetrieb schlichtweg nicht mehr wegzudenken. Aus der Sicht der Auftraggeber ist darauf zu achten, dass im Vertrag mit dem Anbieter Regelungen und Kennzahlen hinsichtlich der Verfügbarkeit des Dienstes nachvollzogen werden können. Das jeweilige Mindestniveau an Verfügbarkeit ist je Organisation und outgesourctem Dienst individuell. Ebenfalls sollte die Zulässigkeit der Einbindung von Subauftragnehmern transparent festgelegt sein. Im Rahmen der Verarbeitung von personenbezogenen Daten (das wird oftmals der Fall sein) durch den Anbieter ist zudem der Abschluss eines Auftragsverarbeitungsvertrags zwingend!

### Implementierung eines Datenschutz-Management-Systems (DSMS)

Um die umfangreichen datenschutzrechtlichen Vorgaben der DS-GVO umsetzen zu können, bietet sich die Implementierung eines DSMS an. Ein solches Managementsystem ermöglicht es, die organisatorischen Rahmenbedingungen für die Erfüllung aller datenschutzrechtlichen Pflichten im Blick zu halten und gleichzeitig insbesondere Rechenschaftspflicht aus Art. 5 DS-GVO zu erfüllen. Dadurch können systematisch die diversen datenschutzrechtlichen Anforderungen erfüllt werden, was gleichzeitig auch der Informationssicherheit dient. Denn die vier Schutzziele der Informationssicherheit decken sich mit den Schutzzielen der DS-GVO im Hinblick auf personenbezogene Daten und vor allen Dingen auch für Gesundheitsdaten.

### Aufbau und Aufrechterhaltung eines Informations-Sicherheits-Management-Systems (ISMS)

IT-Sicherheitsawareness beginnt bei der Leitungsebene. Durch die Implementierung eines ISMS anhand eines Top-Down-Ansatzes kann ein ganzheitliches Ergreifen von Maßnahmen zur Sicherstellung der Informationssicherheit gewährleistet werden. Bei dem Aufbau eines ISMS werden innerhalb einer Organisation entscheidende Prozesse geschaffen und das aktuelle Sicherheitsniveau schrittweise erhöht, um langfristig einen Zugewinn an Sicherheit zu erreichen.

Im Rahmen einer Zertifizierung des ISMS, z.B. nach dem internationalen Standard ISO/IEC 27001, werden die getroffenen organisatorischen Maßnahmen von einem unabhängigen Auditor überprüft, sodass eine langfristige Verbesserung der Informationssicherheit ermöglicht werden kann. Gerade für die Erfüllung der branchenspezifischen Sicherheitsstandards (B3S) für Krankenhäuser ist der Aufbau und die Aufrechterhaltung eines ISMS Pflichtprogramm.

MORGENSTERN

## Bleib bei erforderlichen IT-Sicherheitsmaßnahmen up to date!

Um deine IT-Infrastruktur umfangreich schützen zu können, sind diverse IT-Sicherheitsmaßnahmen erforderlich. Hierbei ist eine regelmäßige Evaluierung der vorhandenen Maßnahmen unabdinglich, sodass im Bedarfsfall weitere Maßnahmen ergriffen werden können.

Um sich vor Schadsoftware zu schützen, sind nicht nur aktuelle Virenscanner ausreichend. Mithilfe einer Applikationskontrolle, die nur das Ausführen von zulässigen Anwendungen zulässt, kann die Ausführung von Schadsoftware verhindert werden. In diesem Rahmen empfiehlt sich ein „Zero Trust"-Ansatz, wodurch nur die aktiv zugelassenen Anwendungen die erforderlichen Berechtigungen erhalten.

Externe Angreifer können mit einem Intrusion Detection System (IDS) erkannt und mit einem Intrusion Prevention System (IPS) automatisiert abgewehrt werden. Dabei stützen sich diese Systeme auf erkannte Verhaltensmuster im eigenen Netzwerk und entwickeln sich damit stetig weiter.

Außerdem ist ein ausgereiftes Update- und Patchmanagement erforderlich, um die im Einsatz befindlichen Anwendungen und Geräte vor neuen Bedrohungen zu schützen. Da sich Angreifer stetig weiterentwickeln und neue Sicherheitslücken entdecken, ist es umso wichtiger, die Mittel, die einem der Hersteller von zertifizierten Softwareprodukten und zertifizierter Hardware zur Verfügung stellt, unmittelbar zu installieren. Eine verzögerte Installation von erforderlichen Sicherheitsupdates kann nämlich von Angreifern direkt ausgenutzt werden – denn wenn Sicherheitsupdates bekannt werden, werden auch die bestehenden Sicherheitslücken bekannt!

Um eine Benutzung der Systeme durch unberechtigte Dritte zu vermeiden, kann zur Authentifizierung der berechtigten Mitarbeitenden eine Multi-Faktor-Authentifizierung (MFA) eingesetzt werden, um die verschiedenen Schutzziele der Informationssicherheit zu erreichen.

## Klassifizieren von betriebskritischen und betriebsrelevanten Systemen und Daten!

Die IT-Sicherheitsmaßnahmen sind besonders wichtig für die betriebskritischen und betriebsrelevanten Systeme und Daten. Aber um überhaupt erst zu wissen, was man mit welchen Sicherheitsmaßnahmen schützen sollte, ist es erforderlich, eine Klassifizierung der entsprechenden Schutzgegenstände durchzuführen. Das dient einerseits der internen Dokumentation, andererseits lassen sich somit aber Priorisierungen bei dem Ergreifen von Schutzmaßnahmen vornehmen. So sollten besonders sensible Daten zwingend verschlüsselt werden, um eine Verletzung der Vertraulichkeit auszuschließen.

MORGENSTERN

# Mehr Sicherheit ...

## ... im Gesundheitswesen

### I. IT-Security im Healthcare-Sektor

- **Basis-Check-Up Package** — ab 1.680,00 EUR zzgl. MwSt.
- **ISMS-Update Package** — ab 1.680,00 EUR pro Tag zzgl. MwSt.

### II. Datenschutz im Healthcare-Sektor

- **Krankenhaus Basis Package** — ab 1.680,00 EUR zzgl. MwSt.
- **Arztpraxis Basis Package** — ab 1.680,00 EUR zzgl. MwSt.
- **IT-Dienstleister Basis Package** — ab 1.680,00 EUR zzgl. MwSt.

**morgenstern-privacy.com**

» **Jetzt Angebot anfordern**

# the future is yours.

**Steigerung der Awareness bei den Mitarbeitenden!**

Nicht nur die technischen Einrichtungen bieten für Angreifer ein attraktives Ziel. Gerade die eigenen Mitarbeitenden werden von Angreifern häufig auserkoren, um Schadcode einzubringen oder um vertrauliche Informationen zu erhalten. Deswegen ist bei allen Beschäftigten ein Sicherheitsbewusstsein dahingehend zu schaffen, dass sie sich aller Risiken bewusst sind und im Ernstfall richtig reagieren können. Hier ist ein enges Zusammenarbeiten mit der eigenen IT-Abteilung ratsam, um auch z.B. auf die Bedrohung von Social-Engineering-Attacken aufmerksam zu machen. Damit wird durch eine umfassende Aufklärung der Mitarbeitenden menschliches Fehlverhalten proaktiv verhindert.

**Informationssicherheit als Bedingung für Cyber-(Pflicht)Versicherungen!**

Während Cyber-(Pflicht)Versicherungen finanzielle Schäden abfangen können, werden in den Versicherungsbedingungen den Versicherungsnehmern in der Regel umfassende Informationssicherheitsmaßnahmen als Obliegenheiten auferlegt. Ansonsten droht im Falle eines Schadenseintritts ein kompletter Ausfall des Versicherungsschutzes. Die Informationssicherheit ist in diesem Falle dann nicht nur ein Selbstzweck, sondern schützt einerseits die eigene Organisation direkt und dient in der Folge der Gewährleistung des Versicherungsschutzes.

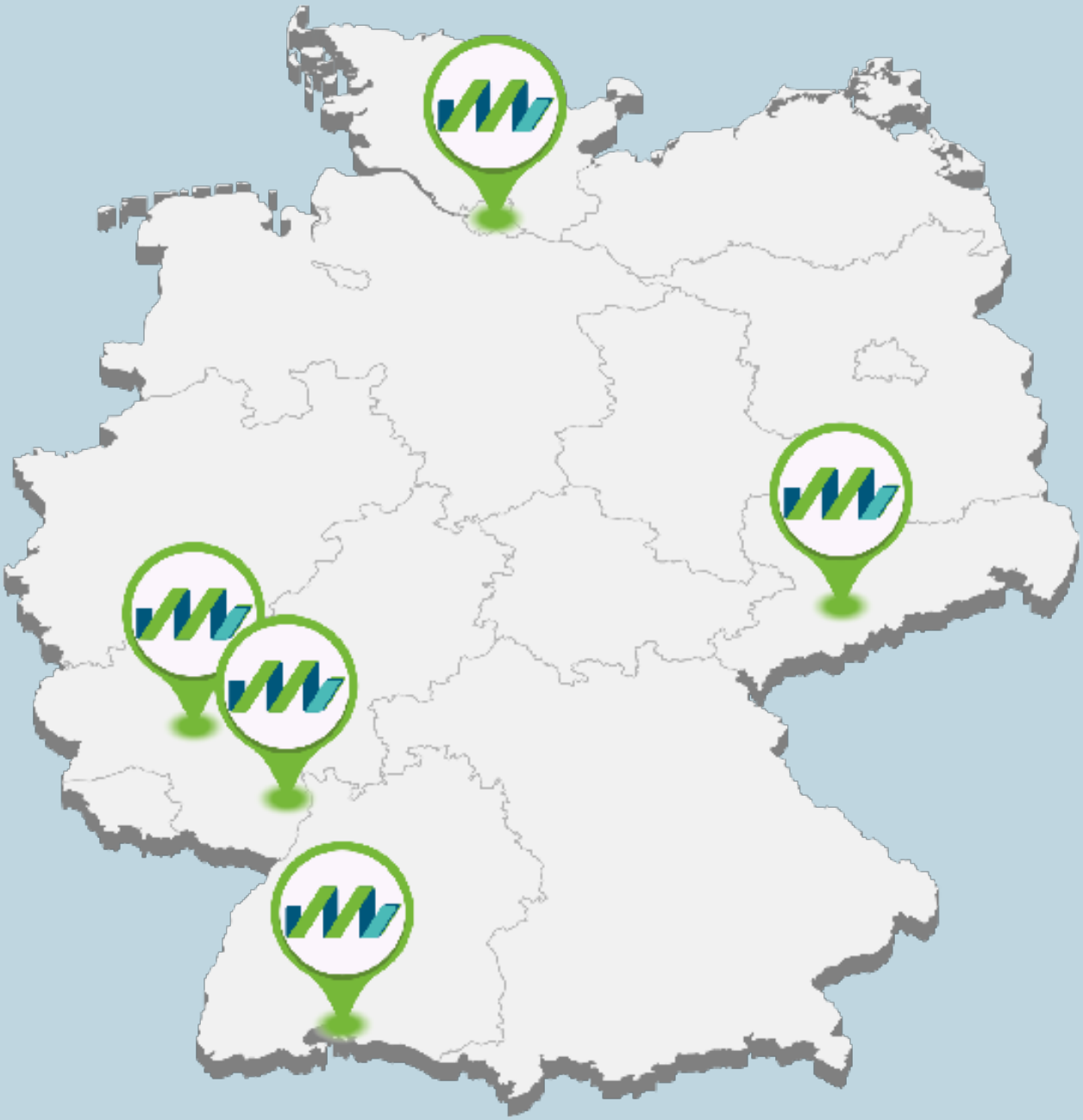
## V. Schlussbemerkung

Eine sicherheits- und datenschutzorientierte Digitalisierung und Innovation im Healthcare-Sektor kann die Nutzung der Potenziale für sämtliche Stakeholder zukunfts- und rechtssicher abbilden. Es lohnt sich daher, auch angesichts zunehmender Bedrohungen und steigender Haftungsrisiken, auf funktionale und praktikable Lösungsansätze zurückzugreifen.

## VI. Learnings

Die Chancen und Potenziale vernetzter Softwareanwendungen und Datensysteme

MORGENSTERN



MORGENSTERN
consecom GmbH

Große Himmelsgasse 1 | D-67346 Speyer
T +49 (0) 6232 - 100119 44
contact@morgenstern-privacy.com