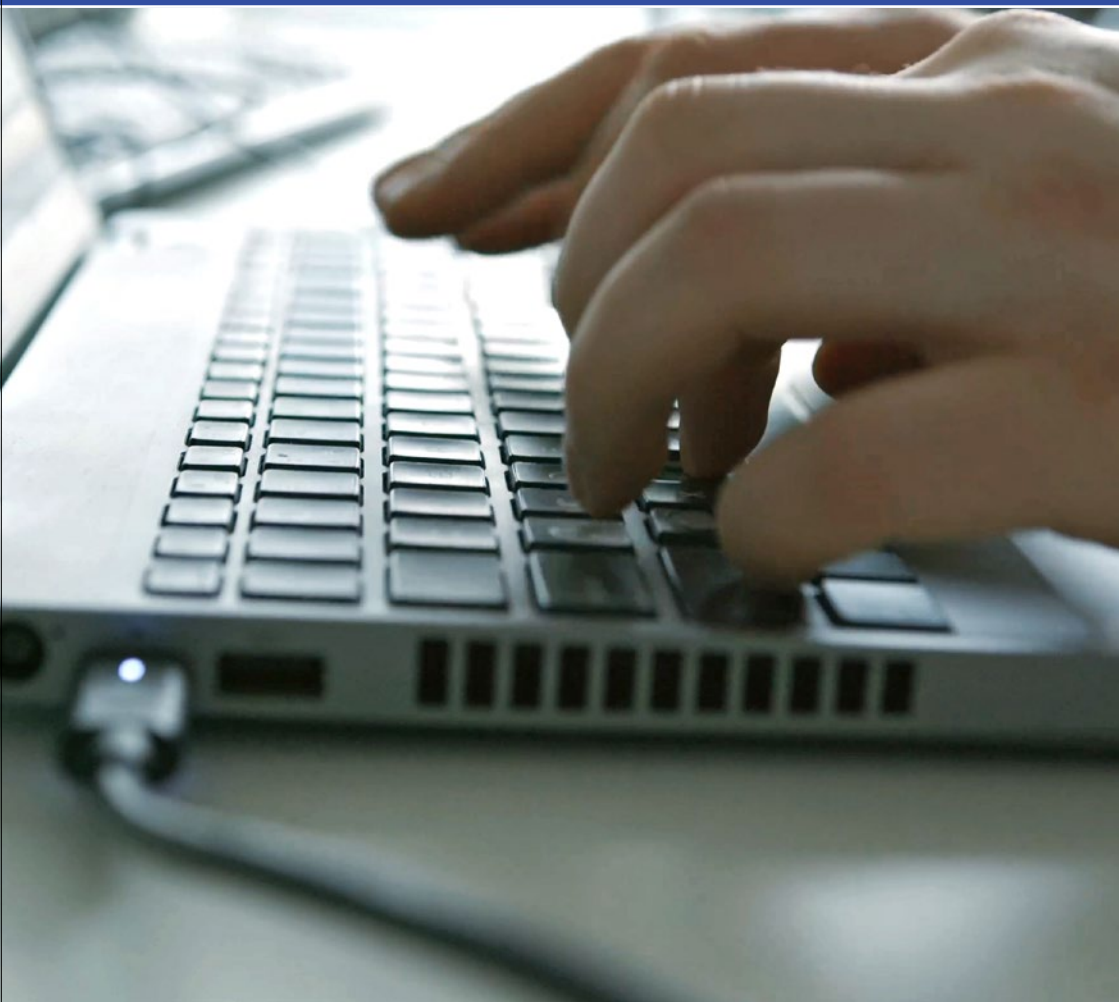
Rödl & Partner

IT-SICHERHEIT IM KRANKENHAUS

BEDROHUNGEN VORBEUGEN



Sicherheit als Grundlage und Rechtspflicht

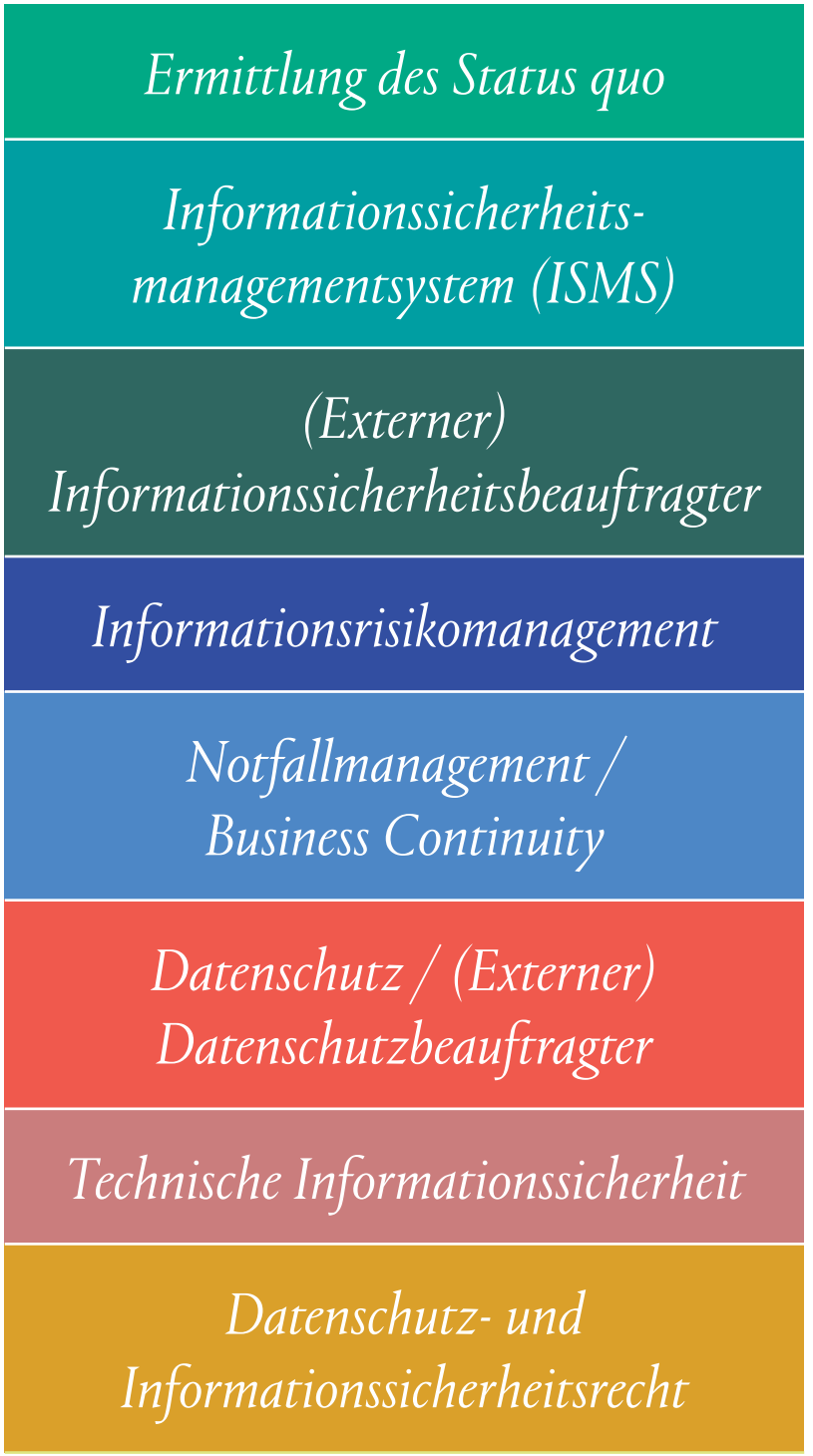
In den letzten Wochen und Monaten sind Cyberangriffe auf Krankenhäuser dramatisch angestiegen. Dabei haben es die Angreifer vor allem auf Schwachstellen in der IT-Infrastruktur abgesehen. Erfolgreiche Angriffe können nicht nur die Informationssicherheit beeinträchtigen sondern auch die Patientensicherheit gefährden.

Aus diesem Grund müssen Krankenhäuser in die Stärkung ihrer IT-Sicherheit investieren, um dieser Bedrohung entgegenzuwirken. Darüber hinaus haben sie auch eine gesetzliche Verpflichtung zur Sicherstellung der IT-Sicherheit im Krankenhaus. Durch § 391 SGB V werden Krankenhäuser zur Umsetzung des Stands der Technik verpflichtet. Dieser bezieht sich auf die aktuellen und bewährten Methoden, Verfahren, Mittel und Maßnahmen im Bereich der Informationstechnologie, die geeignet sind, die Sicherheit und den Schutz von sensiblen Gesundheitsdaten und zur Aufrechterhaltung der Patientenversorgung zu gewährleisten.

Die Maßnahmen gelten als angemessen, solange der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls, einer Beeinträchtigung des Krankenhauses oder dem Schutzbedarf der verarbeiteten Patienteninformationen steht. Da es sich bei Patientendaten um besonders schützenswerte Daten handelt, ist die Messlatte sehr hoch.

Die Krankenhäuser können die Verpflichtungen insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard (B3S) für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus umsetzen.

In dieser Broschüre möchten wir Ihnen einen Überblick geben, wie Sie Ihren Status quo ermitteln und welche Themen Sie im Rahmen der IT-Sicherheit beachten sollten. Dies umfasst insbesondere die folgenden Themenschwerpunkte, die maßgeblich zur Sicherheit und Verfügbarkeit der IT-Systeme beitragen können, sodass es zu keiner Einschränkung in der Patientenversorgung kommt:



Ermittlung des Status quo

Die Durchführung einer Bestandsaufnahme in Form einer Prüfung mit dem Fokus auf die Erfüllung der Anforderungen aus § 391 SGB V ist ein entscheidender erster Schritt, bevor Maßnahmen zur Verbesserung der IT-Sicherheit implementiert werden. Nur so können zielgerichtet die passenden und notwendigen Maßnahmen ergriffen werden:

Schwachstellenidentifikation:

Eine Bestandsaufnahme ermöglicht die Identifikation von technischen Schwachstellen in der bestehenden IT-Umgebung und organisatorischen Mängeln im internen Kontrollsystem, bewertet nach Schweregrad und potentiellem Risiko.

Maßnahmendefinition:

Im nächsten Schritt werden technische und organisatorische Maßnahmen zur Behebung der Mängel und Risiken definiert.

Ressourcenbewertung:

Durch die Bestandsaufnahme lassen sich die vorhandenen Ressourcen, sowohl finanzieller als auch personeller Art, nachvollziehbar bewerten.

Priorisierung von Maßnahmen:

Auf Grundlage der vorhandenen Ressourcen kann eine fundierte Priorisierung der Sicherheitsmaßnahmen erfolgen.

Insgesamt schafft eine umfassende Bestandsaufnahme eine solide Grundlage für die Entwicklung und Implementierung von effektiven IT-Sicherheitsmaßnahmen. Es empfiehlt sich dabei wie bei einer KRITIS-Prüfung nach § 8a BSIG vorzugehen – lediglich der Nachweis der Umsetzung bzw. die Einreichung festgestellter Mängel muss nicht beim Bundesamt für Sicherheit in der Informationstechnik (BSI) erfolgen.

WARUM RÖDL & PARTNER?

Es hilft die vorhandenen Schwachstellen durch einen Prüfer aufgezeigt sowie bewertet zu bekommen und anschließend gemeinsam die Behebungsmaßnahmen zu besprechen. Wir greifen auf die Erfahrung von knapp 20 Jahren IT-Prüfungen in der Gesundheitswirtschaft und einer sehr großen Zahl an KRITIS-Prüfungen zurück und können daher gut einschätzen, wie Häuser im Branchenvergleich aufgestellt sind.

Jürgen Schwestka

Partner

+49 911 9193 3508

juergen.schwestka@roedl.com

Informationssicherheits-managementsystem (ISMS)

KURZ ERKLÄRT:

Die Wichtigkeit eines Informationssicherheitsmanagementsystems (ISMS) ergibt sich aus vielfältigen Faktoren. Der Hauptzweck liegt darin, Organisationen zu helfen ihre sensiblen Informationen vor Bedrohungen zu schützen und gesetzliche Anforderungen zu erfüllen. Gleichzeitig wird das Vertrauen der Stakeholder gestärkt und die Verfügbarkeit von Informationen sichergestellt. Weitere Ziele sind ein besseres Management von Risiken, die Sicherstellung der Verfügbarkeit von Informationen, Schutz der eigenen Reputation, Effizienzsteigerung und kontinuierliche Verbesserung, Erlangung eines Wettbewerbsvorteils und die Reduzierung von Kosten für Sicherheitsvorfälle. Das ISMS bietet somit einen strukturierten Ansatz zur Gewährleistung der Informationssicherheit.

Beim Aufbau des Managementsystems sollten bewährte Standards und Rahmenwerke herangezogen werden.

Weit verbreitete und anerkannte Standards sind insbesondere:

- Branchenspezifischer Sicherheitsstandard der jeweiligen Branche, z.B. B3S „Medizinische Versorgung“ für Krankenhäuser
- ISO/IEC 27001
- IT-Grundschutz des BSI

Bei der Auswahl eines entsprechenden Rahmenwerks oder Standards sollten die spezifischen Anforderungen, Risiken und der Kontext betrachtet werden. Branchenspezifische Besonderheiten müssen dabei im ISMS berücksichtigt werden. Daher empfiehlt sich eine Orientierung am Branchenspezifischen Sicherheitsstandard (B3S).

Außerdem müssen Prozesse zur Überwachung neuer Anforderungen etabliert werden. Aktuelle Änderungen sind z.B. das „NIS2 Umsetzungsgesetz“ zur Stärkung der Cybersicherheit sowie das „KRITIS-Dachgesetz“, welches die Resilienz und physische Sicherheit kritischer Infrastrukturen regelt.

WARUM RÖDL & PARTNER?

Im Rahmen der Durchführung von KRITIS-Prüfungen sind wir mit den Elementen und der Bewertung von ISMS, im Sinne einer Reifegradbeurteilung, bestens vertraut. Darüber hinaus konnten wir bereits viele Mandanten bei der Implementierung von ISMS, bspw. nach B3S oder ISO/IEC 27001 unterstützen und beraten.

Rüdiger Hanke

Manager

+49 911 9193 1410

ruediger.hanke@roedl.com

(Externer) Informationssicherheits-beauftragter

KURZ ERKLÄRT:

Ein Informationssicherheitsbeauftragter (ISB) ist notwendig, um die Entwicklung, Umsetzung und Überwachung von Informationssicherheitsmaßnahmen in einer Organisation zu gewährleisten.

Die interne Besetzung der Position eines ISB in Krankenhäusern kann oftmals eine Herausforderung darstellen. Dies liegt u.a. an folgenden Gründen:

- Die Position erfordert spezifische Kenntnisse im Bereich Informationssicherheit im Gesundheitswesen.
- Die Aufgaben sind sehr umfangreich und können meist nicht neben der normalen Tätigkeit übernommen werden.
- Die Rolle des ISB ist umfangreich und erfordert ein tiefes Verständnis für Datenschutz und Compliance.
- Ein ISB muss Risikomanagement- und Kontrollfunktionen übernehmen, was spezifische Fähigkeiten erfordert, die nicht jeder interne Kandidat besitzt.
- Krankenhäuser haben möglicherweise begrenzte Ressourcen für die Schulung und Weiterbildung von internen Mitarbeitern, um sie auf die Anforderungen der Position vorzubereiten.
- ISB sind in allen Branchen stark begehrt, daher werden sie oft von anderen Branchen abgeworben, die nicht an einen Tarifvertrag gebunden sind.
- Die Bestellung eines externen ISB kann daher eine sinnvolle Lösung für Krankenhäuser sein.

WARUM RÖDL & PARTNER?

Gerne unterstützen wir Sie mit unserer Fachkompetenz und Branchenerfahrung. Unsere ISB haben viele Jahre Erfahrung in der IT-Prüfung und IT-Beratung. Sie werden unterstützt von Datenschutzexperten, Fachanwälten für IT-Recht u.v.m. – Sie haben immer ein Team von Experten in allen Themenbereichen auf Abruf!

Jonas Buckel

Manager

+49 911 9193 3627

jonas.buckel@roedl.com

Informationsrisikomanagement

KURZ ERKLÄRT:

Das Informationsrisikomanagement ist ein Prozess, der darauf abzielt, die Risiken für Informationen in einer Organisation zu identifizieren, bewerten, steuern und überwachen. Einige zentrale Aspekte, die das Informationsrisikomanagement ausmachen sind:

- Identifikation von Informationsrisiken
- Bewertung von Informationsrisiken
- Risikobehandlung
- Implementierung von Sicherheitskontrollen
- Überwachung und Überprüfung
- Dokumentation und Berichterstattung
- Kontinuierliche Verbesserung
- Kommunikation und Sensibilisierung
- Integration in das Gesamt-Risikomanagement
- Compliance mit Standards und Vorschriften

Ein effektives Informationsrisikomanagement ist entscheidend, um die Sicherheit von Informationen zu gewährleisten und die Geschäftskontinuität in einer zunehmend digitalisierten Welt zu schützen.

Es trägt dazu bei, sicherzustellen, dass Informationsrisiken auf akzeptable Niveaus reduziert werden und die Organisation widerstandsfähig gegenüber Sicherheitsbedrohungen bleibt.

WARUM RÖDL & PARTNER?

Krankenhäuser profitieren bei uns davon, dass wir mehrjährige Erfahrung in der Umsetzung und Betreuung von Risikomanagement-Systemen bei Unternehmen der Gesundheitswirtschaft einbringen und dabei in Bezug auf einzusetzende technische Tools anbieterunabhängig sind.

Katja Pfannenmüller

Associate Partner

+49 911 9193 1127

katja.pfannenmueller@roedl.com

Notfallmanagement / Business Continuity

KURZ ERKLÄRT:

Notfallmanagement ist wichtig, da es ermöglicht, im Ernstfall schnell und effektiv zu reagieren. Sollte es zu einem Notfall kommen, müssen Notfallpläne bereits fertiggestellt und ihre Wirksamkeit idealerweise auch erprobt worden sein.

Ein strukturiertes Notfallmanagement ...

- sichert die Geschäftskontinuität,
- minimiert Risiken,
- schützt Mitarbeiter und Vermögenswerte,
- umfasst effektive Notfallkommunikation,
- fördert die Wiederherstellung von IT-Systemen und
- ermöglicht kontinuierliche Verbesserung.

Es ist elementar für die Sicherstellung der medizinischen Versorgung im Krankenhaus!

Um das Risiko für die Gesundheitsversorgung möglichst gering zu halten, gilt es u.a. auch, sich auf den Notfall vorzubereiten und notwendige organisatorische und technische Maßnahmen umzusetzen. Hierzu gehören mit unter die klassischen IT-Aufgaben: z.B. aktuelle Patch-Stände auf den IT-Systemen, strenge Firewall-Regeln, Systeme zur Angriffserkennung und -verhinderung, aktuelle Virenschutzsysteme, aber auch ausreichend sensibilisierte Mitarbeiter.

Doch trotz aller Vorsichtsmaßnahmen lässt sich ein professioneller Angriff oft nicht verhindern. Es gilt daher möglichst gut vorbereitet zu sein, falls es doch einmal passiert.

Stellen Sie sich die folgenden Fragen, um den Stand Ihrer bisherigen Vorbereitung abzuschätzen:

1. Wie funktioniert die Kommunikation, wenn die IT-Systeme ausgefallen sind?
2. Welche Bereiche müssen in das Notfallmanagement eingebunden sein?
3. Wer kann im Falle eines Notfalls unterstützen?

Wenn Sie zu diesen Fragen noch keine finalen Antworten und nachvollziehbare Pläne haben, sollten Sie kritisch über Ihr bisheriges Notfallmanagement nachdenken!

WARUM RÖDL & PARTNER?

Sie profitieren neben pragmatischen IT-Lösungsansätzen auch von unseren Erfahrungen im Krisenmanagement. Krisen wirken sich in der Regel nicht nur auf isolierte Bereiche (z.B. IT), sondern auf das gesamte Krankenhaus als Einheit aus. Wir unterstützen Sie beim Aufbau & Betrieb eines ganzheitlichen Notfallmanagements sowohl vor, während, als auch nach der Krise.

Nils Mensel

Senior Associate

+49 911 9193 3618

nils.mensel@roedl.com

Datenschutz / (Externer) Datenschutz-beauftragter

KURZ ERKLÄRT:

Informationssicherheit und Datenschutz müssen eng zusammenarbeiten, da beide Disziplinen das gemeinsame Ziel haben, die Sicherheit von Informationen zu gewährleisten und deren unrechtmäßigen Zugriff der unautorisierten Verwendung zu verhindern.

Das Zusammenspiel der beiden Themen ermöglicht eine umfassende Identifikation, Bewertung und Minderung von Risiken im Zusammenhang mit personenbezogenen Daten und anderen sensiblen Informationen. So muss z.B. bei der Einführung neuer Anwendungen stets geprüft werden, welche Auswirkungen dies auf die Informationssicherheit hätte und unter welchen Bedingungen Anwendungen datenschutzkonform verwendet werden können. Besonders herausfordernd wird es, wenn es sich dabei um Cloud-Anwendungen oder KI-Software handelt.

Auch bei der Beurteilung von Sicherheitsvorfällen ist eine durchgängige Abstimmung notwendig, zumal hier verschiedene Meldepflichten gegenüber dem BSI, Datenschutzbehörden oder weiteren Behörden bestehen können.

Die enge Zusammenarbeit zwischen Datenschutz und Informationssicherheit ist somit entscheidend, um einen ganzheitlichen Ansatz für den Schutz von Informationen, insbesondere personenbezogenen Daten, zu gewährleisten.

WARUM RÖDL & PARTNER?

Durch unsere jahrelangen Erfahrungen als externer Datenschutzbeauftragter können wir Sie bei diesem Thema ebenfalls umfassend beraten und unterstützen.

Sofern Sie in diesem Zusammenhang beabsichtigen, die Verantwortung des Datenschutzbeauftragten nach Extern zu verlagern, können wir auch gerne einen unserer qualifizierten Mitarbeiter für diese Aufgabe stellen.

Zusätzlich dazu konnten wir in der Vergangenheit auch umfassende Erfahrungen in datenschutzrechtlichen Konfliktsituationen zwischen Krankenhäusern und der jeweils zuständigen Datenschutzaufsichtsbehörde sammeln.

Denise Klante

Senior Associate

+49 911 9193 1178

denise.klante@roedl.com

Technische Informationssicherheit

KURZ ERKLÄRT:

In der technischen Informationssicherheit gibt es verschiedene Gefahren und Bedrohungen, die die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen gefährden können.

Hier sind einige der häufigsten Gefahren:

- Cyber-Angriffe
- Malware bzw. Schadprogramme
- Schwachstellen in Software und Systemen
- Unsichere Konfigurationen
- Unzureichende Absicherung des Netzwerks
- Schatten-IT
- Veraltete Systeme

Um sich gegen diese Gefahren zu schützen, ist es entscheidend, ausreichende und aktuelle Sicherheitsmaßnahmen wie Angriffserkennung, Antivirensoftware, Schwachstellenscanner, standardisierte Konfigurationsvorgaben, Firewallsysteme, Inventarisierung, regelmäßige Sicherheitsupdates und Schulungen für Mitarbeiter zu implementieren.

Ein umfassender Ansatz zur technischen Informationssicherheit ist somit notwendig, um die Risiken zu minimieren und die Widerstandsfähigkeit gegenüber Cyberbedrohungen zu stärken.

WARUM RÖDL & PARTNER?

Mit unserem Fachwissen führen wir intensive technische IT-Prüfungen durch, um eventuell vorhandene Schwachstellen aufzudecken und Ihnen den Handlungsbedarf darzulegen.

Gemeinsam werden wir die vorgefundenen Schwachstellen bewerten und deren Behebung priorisieren. Dabei geben wir auch gerne praktische Tipps zur Umsetzung.

In diesem Zusammenhang können wir auf die Erfahrungen aus 20 Jahren in den Bereichen IT-Administration und IT-Sicherheit zurückgreifen.

Matthias Edler

Manager
+49 30 810795 7050
matthias.edler@roedl.com

Datenschutz- und Informations-sicherheitsrecht

KURZ ERKLÄRT:

Praktische Umsetzungen können nur dann sicher erfolgen, wenn diese auch auf die rechtlichen Rahmenbedingungen abgestimmt sind.

So ist beispielsweise eine Auslagerung in die Cloud nur erlaubt, wenn das Krankenhaus selbst den Stand der Technik umsetzt (vgl. § 391 SGB V) und der Cloud-Anbieter als datenverarbeitende Stelle über ein aktuelles C5-Testat verfügt (vgl. § 393 SGB V).

Eine rechtskonforme Ausgestaltung der Sicherheitsmaßnamen sowie des Datenschutzes ist aber auch Voraussetzung um Haftungstatbestände im Falle eines Angriffes bestmöglich zu vermeiden. In diesem Zusammenhang ist es besonders wichtig immer zeitnah über gesetzliche Änderungen informiert zu sein, um notwendige Anpassungen durchführen zu können.

Aber auch nach einem Cyberangriff gilt es nicht nur schnell, sondern auch gesetzeskonform zu handeln. Hier stellen sich die Fragen wer, wie, über welche Tatsachen zu informieren ist.

WARUM RÖDL & PARTNER?

Wir können in beiden Fällen nicht nur beratend tätig werden, sondern auch Sie und Ihre Mitarbeiter bezüglich der Anforderungen schulen, um eine höhere Sensibilisierung zu schaffen und so Fehler zu vermeiden.

Aufgrund der Tatsache, dass wir hier eng mit den praktisch tätigen Kollegen zusammenarbeiten, geben wir nicht nur starre rechtliche Auskünfte, sondern beziehen die tatsächlich bei Ihnen vor Ort vorliegenden Gegebenheiten und die Möglichkeiten der praktischen Umsetzung direkt in unsere Beratung mit ein. Sie erhalten daher ein Komplettpaket und müssen sich nicht zusätzlich noch an weitere Stellen wenden.

Carina Richters

Manager

+49 221 949 909 206

carina.richters@roedl.com

Herr Schwestka ist seit knapp 20 Jahren im Bereich der Gesundheits- und Sozialwirtschaft aktiv. Er beschäftigt sich intensiv mit den Themen Digitalisierung und Informationssicherheit.

Neben der Seite Prüfer- und Beratersicht, kennt er auch den „Blick von Innen“: Herr Schwestka ist seit fast 5 Jahren externer ISB bei einem Unternehmen der Kritischen Infrastruktur in der Gesundheitswirtschaft.

Es ist wichtig beide Seiten zu kennen, damit pragmatische Ansätze gefunden werden, die einerseits sicher sind, andererseits die Arbeit aber nicht allzusehr einschränken.

Herr Hanke ist seit über 12 Jahren im Bereich IT-Audit und IT-Beratung tätig. Hierbei war er maßgeblich bei der Einführung von ISMS nach CISIS12 im kommunalen Umfeld beteiligt und war gleichzeitig als stellvertretender externer Informationssicherheitsbeauftragter (ISB) tätig. Herr Hanke ist langjähriger KRITIS Prüfer und verfügt über eine große Expertise im Bereich von Informationssicherheitsstrukturen im Krankenhausumfeld.

Über mehrere Jahre hinweg betreute Herr Hanke federführend den Bereich IT-Governance bei einem der größten deutschen Versicherungsunternehmen.

Herr Buckel ist seit über 5 Jahren im Bereich der Gesundheits- und Sozialwirtschaft aktiv. Er beschäftigt sich intensiv mit dem Thema Informationssicherheit und ist seit über 4 Jahren als externer ISB bei einem Unternehmen der Kritischen Infrastruktur in der Gesundheitswirtschaft bestellt.

Neben der beratenden Tätigkeit führt Herr Buckel noch Prüfungen von kritischen Betreibern nach § 8a BSIG durch. Somit hat er den „Blick von Innen“, um pragmatische Lösungen umzusetzen, und kennt auch alle gesetzlichen Anforderungen, die erfüllt werden müssen.

Frau Pfannenmüller beschäftigt sich seit knapp 15 Jahren mit der Konzeption und Implementierung von Risikomanagementsystemen. Neben der Beratersicht verfügt sie über langjährige Erfahrung auf Unternehmensseite sowohl im Mittelstand als auch im DAXUmfeld.

Die Erfahrungen als Implementierungsverantwortliche auf Unternehmensseite sind wichtig, um pragmatische und wirksame Lösungen etablieren zu können.

Herr Mensel ist seit Januar 2008 bei Rödl & Partner im Bereich der Gesundheits- und Sozialwirtschaft tätig. Zu seinen Kernthemen zählen die Prüfung bzw. die Optimierung des Notfallmanagements / Business Continuity sowie der Bereich der Internen Revision.

Im Rahmen zahlreicher Revisionsprüfungen wurden häufig Schwachstellen im Notfallmanagement identifiziert bzw. wurden Interne Revisionen nach eingetretenen Notfällen zur Identifikation der Ursachen beauftragt. Die Erfahrung zeigt deutlich: „Vorsorge ist günstiger als Nachsorge“.

Frau Klante ist als Wirtschaftsjuristin und zertifizierte Datenschutzbeauftragte für Mandanten in der Gesundheits- und Sozialwirtschaft vor allem für Datenschutz-Fragestellungen zuständig.

Neben Tätigkeiten in Prüfungs- und Beratungsaufträgen übernimmt Frau Klante ebenso die Funktion als externe Datenschutzbeauftragte. Aufgrund ihrer mehrjährigen Erfahrung in der Gesundheitswirtschaft kennt Frau Klante die datenschutzrechtlichen Herausforderungen, die sich innerhalb eines Krankenhauses ergeben und unterstützt unsere Mandanten insofern bei der praxisnahen und lösungsorientierten Umsetzung des Datenschutzes.

Herr Edler und sein Team beraten Sie zu sämtlichen Themen der IT-Sicherheit in der Gesundheits- und Sozialwirtschaft.

Mit 20 Jahren Berufserfahrung in der IT-Administration / IT-Infrastruktur und zuletzt circa 5 Jahren als IT-Sicherheitsbeauftragter sowie Teamleiter IT-Systemtechnik bringt er umfangreiches Wissen aus dem IT-Alltag mit. Mit diesem Know-How können wir Ihnen pragmatische technische und organisatorische Lösungen an die Hand geben.

Frau Richters ist seit über 13 Jahren als Rechtsanwältin tätig und berät Mandanten in der Gesundheits- und Sozialwirtschaft schwerpunktmäßig in Datenschutz- und Informationssicherheitsrechtlichen Fragen.

Durch ihre frühere Tätigkeit als Datenschutzkoordinatorin in einem Versicherungsunternehmen kann sie Erfahrungen auch auf „der anderen“ Seite aufweisen und schaut somit auch mit einem praktischen Blick auf rechtliche Fragestellungen. Dies ist wichtig um praxisnahe Lösungsansätze anbieten zu können.

Über uns

Rödl & Partner prüft und berät seit dem Jahr 1993 mit der Geschäftseinheit „Gesundheits- und Sozialwirtschaft“.

MIT RUND 140 KOLLEGINNEN UND KOLLEGEN AUS DEN BEREICHEN ...

- Wirtschaftsprüfung
- Steuerberatung
- Rechtsberatung
- Unternehmensberatung
- IT-Prüfung und IT-Beratung

... KÖNNEN WIR UNSERE MANDANTEN UMFASSEND UND IN NAHEZU ALLEN FRAGESTELLUNGEN UNTERSTÜTZEN.

Besuchen Sie uns online:

https://www.roedl.de/assurance-it

Oder buchen Sie einen Termin unter:

https://bit.ly/bookwithme-js