KuBuS® – digitale Sicherheit für das Heilwesen

Cyber-Versicherung

Vertrauen, das bleibt.

Die Continentale

Volle Konzentration auf Ihre Patienten

Mit Ihrer Berufswahl haben Sie sich dem Dienst am Menschen verschrieben und übernehmen damit eine sehr wichtige gesellschaftliche Funktion. Während Sie sich primär um das Wohl Ihrer Patienten kümmern, schützt und begleitet Sie die KuBuS® Cyber-Versicherung umfassend bei digitalen Angriffen auf Ihre Praxis.

„Mit KuBuS® im Rücken kann ich mich voll und ganz meinen Patienten widmen."

Digital ist das neue Analog

Wie digital ist Ihre Praxis?

In Ihrer Praxis verwalten Sie seit jeher hochsensible Gesundheitsdaten Ihrer Patienten. Die zunehmende Digitalisierung erleichtert Ihnen zwar vieles, macht Sie aber auch anfällig für Cyber-Attacken. Davon können neben der Patientenverwaltung auch die Abrechnungssysteme und Ihr Terminmanagement betroffen sein.

Außendarstellung
Die Website wird zum digitalen Praxisschild. Alle Informationen rund um die Praxis und zum Leistungsangebot finden sich im Internet.

Kommunikation
Die Nachfrage nach Online-Terminbuchung und Online-Beratung steigt. Bescheinigungen und Rezepte werden oft elektronisch verschickt.

Digitales Patientensystem
Patientendaten und Befunde werden auf elektronischen Wegen ausgetauscht und gespeichert. Sie unterliegen hohen Anforderungen an den Datenschutz.

Medizinische Ausstattung
Häufig sind moderne Behandlungsgeräte online gesteuert oder unterstützt. Über das Internet erfolgen regelmäßige Updates.

Praxisorganisation
Der Trend geht immer mehr in Richtung papierloses Arbeiten. Administrative Abläufe und das Personalmanagement sind digital einfacher und schneller organisiert.

Finanzverwaltung
Abgerechnet wird mit den Kostenträgern überwiegend elektronisch. Und auch das bargeldlose Zahlen ist für Patienten inzwischen gang und gäbe.

Gute Gründe
für **KuBuS®**

Cyber-Kriminalität kann jeden treffen.

Hacker suchen nicht gezielt nach Opfern. Sie versenden E-Mails in großen Mengen, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu erhöhen. Es geht dabei selten um zielgerichtete Attacken. Die Unternehmensgröße steht dabei nicht im Vordergrund. Deshalb kann jeder zum Ziel werden.

Die vier häufigsten Szenarien im Gesundheitswesen

Medizinische Praxen haben selten ein hohes Budget für die IT-Sicherheit. Das macht sie besonders anfällig für Cyber-Angriffe. Im Bereich der Heilberufe drohen vor allem diese Gefahren:

Hacker erbeuten Patientendaten
Unbekannte verschaffen sich mittels einer Schadsoftware Zugang zu Ihrer Praxisverwaltung. Sie stehlen sensible Patientendaten und bieten diese im Darknet an. Die Kosten für die Wiederbeschaffung, die gesetzlichen Informationspflichten und die Abwehr eines Reputationsschadens betragen je Patientenakte in etwa 150 Euro.

Ransomware
Versehentlich klicken Sie auf einen infizierten E-Mail-Anhang und Ihr Computersystem wird verschlüsselt. Der Erpresser fordert von Ihnen für die Freigabe ein Lösegeld, das Sie nicht zahlen wollen. Die beauftragten IT-Forensiker benötigen drei Tage, um Ihnen den vollen Zugriff auf Ihre Daten wieder zu ermöglichen.

Gekaperte Website
Cyber-Betrüger manipulieren Ihre Website. Sie verbreiten fingierte Meldungen im Namen Ihrer Praxis und sabotieren Ihre Online-Terminverwaltung. Ihr IT-Dienstleister hat für solche Notfallsituationen keine ausreichende Erfahrung. Daher werden externe Sachverständige eingeschaltet, um die Ursache zu ermitteln und den Schaden an Ihrer Website zu beseitigen.

E-Mail an falschen Verteiler
Ihre Mitarbeiterin schickt versehentlich Informationen über Patientenabrechnungen statt an die Krankenkasse an einen externen E-Mail-Verteiler. Sie müssen alle betroffenen Patienten sowie die Datenschutzbehörde informieren. Darüber hinaus ist eine Beratung durch einen Fachanwalt erforderlich.

Das kostet ein Angriff.

Der Fall: Hacker attackieren die IT-Systeme Ihrer Praxis. Sie kopieren Patientendaten und versprechen, gegen die Zahlung von Lösegeld auf die Veröffentlichung der Daten im Darknet zu verzichten.

Info

Nur wenige IT-Dienstleister sind für einen Notfall- oder Kriseneinsatz bei einem Cyberangriff ausgebildet und haben genügend Erfahrung.

Informationspflicht
Information an Patienten und Datenschutzbehörde mit Hilfe eines Rechtsanwalts
Informationskosten 4.000 Euro
Anwaltskosten 2.000 Euro

IT-Forensik
Suche nach Schwachstelle und Bereinigung des IT-Systems durch Spezialisten
Kosten für IT-Forensik 5.000 Euro

Bußgeld
Verhängung eines Bußgeldes durch Behörde aufgrund des vermeidbaren Datenlecks
Bußgeld: 2.500 Euro (nicht versichert)

Schadenersatz
Forderung von Betroffenen nach Veröffentlichung gestohlener Gesundheitsdaten
Schadenersatz 20.000 Euro

Vertrauenskrise
Drohender Imageverlust und Patientenabgang nach Bekanntwerden des Datendiebstahls
Krisenkommunikation 1.000 Euro

Betriebsunterbrechung
Schließung der Praxis bis die IT-Schwachstellen geschlossen sind
Kosten für 2 Tage 5.000 Euro

Im Ernstfall an Ihrer Seite

KuBuS® Cyber unterstützt Sie im Kampf gegen die digitale Kriminalität mit wertvollem Notfall- und Krisenmanagement und schnellen Leistungen im Schadenfall. Drei starke Säulen schützen vor finanziellen und rechtlichen Folgen sowie vor Reputationsschäden.

1. Service-Kosten

Ein Expertenteam begleitet Sie in der Krise und hilft Ihnen, diese schnellstmöglich zu bewältigen, zum Beispiel durch Ermitteln der Ursache, technische Sofortmaßnahmen sowie Erfüllen der gesetzlichen Informationspflichten.

2. Drittschäden

Werden Ansprüche wegen einer Verletzung der Informationssicherheit gegen Sie erhoben, übernehmen wir Ihre rechtliche Vertretung, prüfen, ob die Ansprüche berechtigt sind und leisten Schadenersatz ohne „wenn und aber“.

3. Eigenschäden

Kommt Ihre Praxis durch einen Cyberangriff zu Schaden oder muss sie sogar geschlossen werden, erstatten wir unter anderem Löhne und Gehälter, entgangenen Betriebsgewinn und die Kosten für die Wiederherstellung von Daten.

KuBuS® Cyber im Überblick

	Tarif XXL
Service-Kosten	
Kosten für Soforthilfe (Notfall- und Krisenunterstützung)	✓
Schadenfeststellkosten (Datenforensik)	✓
Benachrichtigungskosten (z. B. gegenüber Kunden)	✓
Abwehr- und Minderungskosten für angedrohte Angriffe auf elektronische Daten	✓
Übernahme von Callcenter-Leistungen	✓
Krisenkommunikation und PR-Maßnahmen	✓
Überwachungs- und Monitoring-Dienstleistungen bei vermutetem Missbrauch von Kundendaten (Kreditkarten- und Bankdaten)	✓
Täterermittlung (z. B. im Fall der Betriebsspionage)	+
Drittschäden	
Persönlichkeits-, Namens-, Urheber- und Markenrechtsverletzungen sowie daraus resultierende Verstöße gegen das Wettbewerbsrecht	✓
Freistellung von Vertragspartnern aus der beauftragten Datenverarbeitung	✓
E-Payment – Vertragsstrafen durch Verletzung von Datensicherheitsstandards	✓
Abwehrkosten bei behördlichen Verfahren	✓
Schadenersatzansprüche von Vertragspartnern wegen vergeblicher Aufwendungen	✓
Abwehr von Unterlassungs- und Widerrufklagen	+
Eigenschäden	
Betriebsunterbrechung oder -beeinträchtigung	✓
Wiederherstellung von Daten	✓
Kosten für Dienstleister zur Sicherheitsanalyse und -verbesserung	✓
Schadenminderungskosten	✓
Mehrkosten durch rechtswidrige Telefonie	✓
Cyber-Erpressung	+
Cyber-Betrug	+
Betriebsunterbrechung nach Ausfall eines Cloud-Dienstleisters	+
Sachschäden an der Hardware der IT-Systeme	+
Erweiterte Rückwärtsdeckung bis zu 3 Jahre vor Versicherungsbeginn*	

✓ = versichert - = nicht versichert + = optional mitversicherbar * = gilt für den Service-Kosten-, Dritt- und Eigenschadenbaustein.

Diese Informationen geben Ihnen einen ersten Überblick zum Leistungsumfang der Versicherung und beruhen auf den Tarifkonditionen Stand 06/2022. Maßgebend sind die Versicherungsbedingungen.

Unverzichtbarer Schutz für das Heilwesen

Ihre Praxis ist Ihre berufliche Existenz. Sie braucht einen umfassenden Schutz, auf den Sie sich verlassen können. Im Analogen, wie im Digitalen. So sind Sie im Heilwesen von Cyber-Angriffen besonders bedroht, da Sie sensible Informationen wie personenbezogene Gesundheitsdaten verwalten, die äußerst schutzbedürftig sind. Mit den drei starken Säulen der KuBuS® Cyber-Versicherung wappnen Sie sich bestens für den Kampf gegen die digitale Kriminalität und möglichen Folgen.

Vertrauen, das bleibt.

Die Continentale Sachversicherung AG ist Teil des Continentale Versicherungsverbundes, einem der großen deutschen Versicherer. Ein typischer Versicherungskonzern ist der Verbund jedoch nicht. Denn bereits seit der Gründung der Muttergesellschaft im Jahre 1926 ist er ein „Versicherungsverein auf Gegenseitigkeit". Daher stellt er die Menschen und ihre Bedürfnisse in den Mittelpunkt.

Nur so kann der Verbund seinen Ansprüchen treu bleiben und nachhaltige Transparenz, Sicherheit und Stabilität bieten. Oder wie wir es nennen: Vertrauen, das bleibt.

S.5e.4740/06.2022

Die Continentale

Continentale Sachversicherung AG
Ruhrallee 92
44139 Dortmund
www.continentale.de

Ein Unternehmen des Continentale Versicherungsverbundes auf Gegenseitigkeit