# SentrySuite® Software Produktsicherheit

## Digitale Bedrohungen in der Pneumologie

SENTRYSUITE® SOFTWARE

vyaire™ MEDICAL

# Weltweite Cyberkriminalität

Die Anzahl von Cyberattacken ist im Vergleich zum Vorjahr um **60%** angestiegen,

**470%** mehr Patientendaten waren betroffen. [1]

Ein EINZELNER PATIENTENDATENSATZ ist bis zu **$1000** wert! [2]

$ $ $

**Die Behebung eines Cyberangriffs ist kostspielig und führt bis zur Behebung zu anhaltenden Umsatzeinbußen.** [3]

**Nach durchschnittlich 16 Tagen ist ein betroffenes Netzwerk wieder hergestellt.** [4]

## Das Risiko von sensiblen Daten

Während der Diagnose und Behandlung eines Patienten wird eine große Menge an sensiblen Daten gesammelt und gespeichert, ohne dass besondere Vorsichtsmaßnahmen getroffen werden. Moderne Diagnosegeräte erhöhen die Menge der erfassten, sensiblen Daten und integrieren die Daten anderer Diagnosegeräte, während sie für ganzheitliche Diagnosen unverzichtbar sind.

Patientendaten sind auf dem Schwarzmarkt sehr wertvoll und machen medizinische Anbieter zu primären Zielen für Hacker. Mediziner unterschätzen das Potenzial von regulatorischen und kommerziellen Auswirkungen sowie den Vertrauens- und monetären Verlust, ausgelöst durch Sicherheitsprobleme.

# 16 Tage um Ihr Netzwerk nach einem Ransomware-Angriff wiederherzustellen

## STELLEN SIE SICH VOR, IHR LABOR IST NUR EINEN TAG LANG GESCHLOSSEN

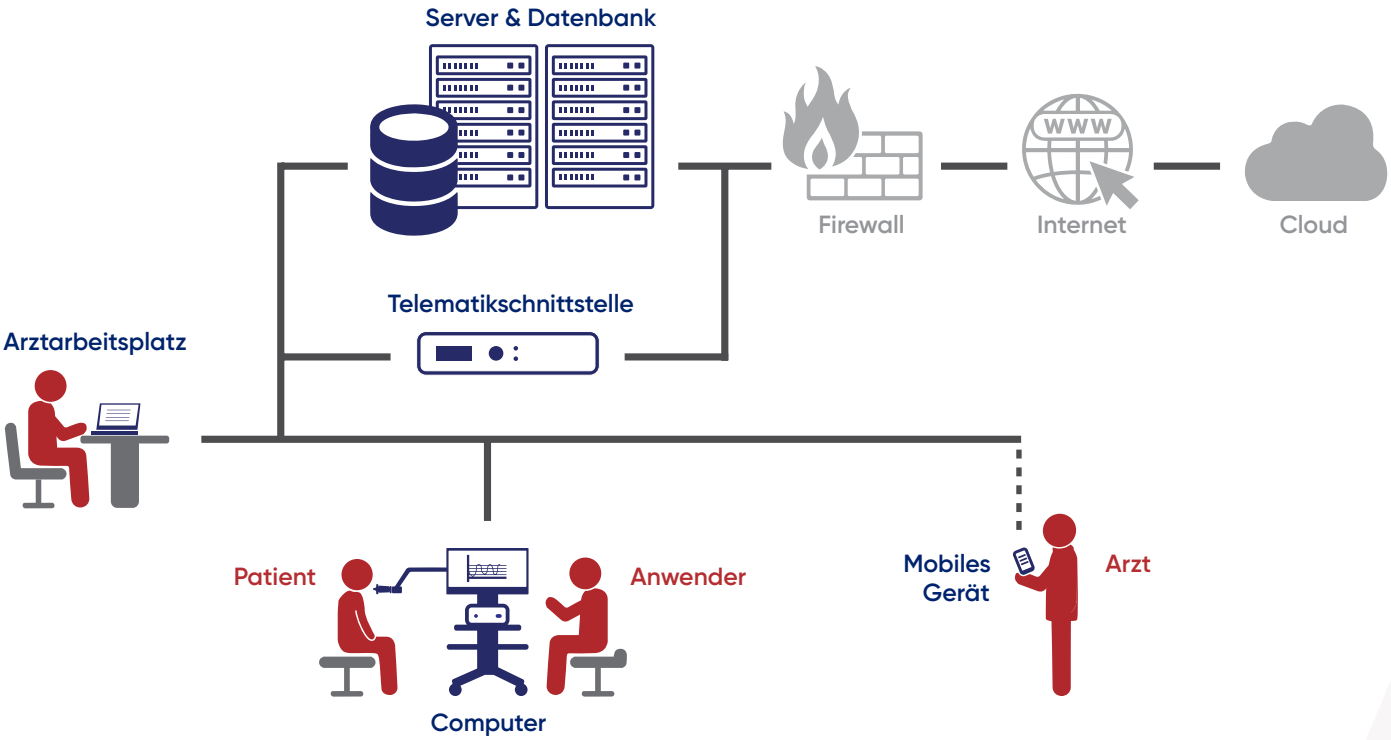
- Sie müssen alle Patienten nach Hause schicken
- Je nach dem Zeitpunkt Ihrer letzten Datensicherung können Sie Daten verlieren
- Sie können Patienten verlieren und Ihre Vertrauen leidet

## DIE LABORSCHLIESSUNG FÜHRT ZU...

- Einem Risiko für den Gesundheitszustand von chronisch kranken Patienten
- Einem Vertrauensverlust, Verlust von Patienten und dem Verlust von Geld
- Laufenden Fixkosten ohne Einnahmen
- Wiederholung von diagnostischen Tests wenn Daten verloren wurden

Die Bedrohung für Ihr Labor ist real. Cyberattacken stellen ein Risiko für die Gesundheit Ihrer Patienten dar und haben einen enormen Einfluss auf Ihre Wirtschaftlichkeit. Bestehende Praxisausfallversicherungen decken oft nicht den Fall von Laborausfällen durch Cyberangriffe ab und IT-Experten berichten häufig von Schwierigkeiten bei der Wiederherstellung des Netzwerks.

# Ein typisches, vernetztes Lungenfunktionslabor




Labore können nur so sicher sein wie ihr schwächster Bestandteil. Elemente eines Labors oder Netzwerks sind nicht nur die medizinischen Geräte, Computer, Server oder mobilen Geräte, sondern auch Bediener, Ärzte, Patienten sowie die Netzwerk- und IT-Infrastruktur sind kritische Bestandteile eines sicheren Labors.

Um ein nachhaltig sicheres System aufzubauen, ist es wichtig, die richtigen Partner zu finden, egal ob es sich um ein isoliert betriebenes System oder ein ganzes vernetztes Labor mit einer Online-Cloud-Anbindung handelt.

# Die richtigen Fragen an Ihren Medizintechnik- oder IT-Lieferanten

Da ein sicheres Labor aus Komponenten verschiedener Hersteller besteht, müssen alle Entscheidungsträger in der Lage sein, die richtigen Partner auszuwählen. Ein Verständnis für potenzielle Gefahren und Bedrohungen innerhalb eines typischen Laboraufbaus ist essenziell. Dazu gehören auch Fragen, die potenziellen Partnern gestellt werden können, um deren Bemühungen in Bezug auf die Produktsicherheit zu verstehen.

Welcher Gefahr sind Sie ausgesetzt?

Welche Bedrohungen können von der Gefahr ausgehen, wenn diese nicht behoben wird?

Wie die Vyaire und SentrySuite Software diese Gefahren für Sie adressiert

Fragen, die Sie dem Anbieter Ihrer aktuellen Lösung stellen können

Personen können auf sensible Daten ohne eine Lese- oder Schreibberechtigung zugreifen.

Sensible Daten könnten eingesehen, manipuliert oder gestohlen werden.

Vyaire SentrySuite unterstützt individuelle Konten für jeden Ihrer Benutzer. Konten können mit starken Passwörtern geschützt werden. Um sicherzustellen, dass Passwörter dem von Ihnen gewüschtem Standard entsprechen, können Sie Anforderungen an die Komplexität der Passwörter definieren.

Außerdem unterstützt SentrySuite die Benutzerauthentifizierung mit einem externen Benutzerverzeichnis wie LDAP oder Windows Active Directory. Damit können Ihre Benutzer ihre bestehenden Konten verwenden, um sich bei unserer Lösung anzumelden.

Unterstützt Ihre Lösung eindeutige Benutzerkonten mit starken Passwörtern und eine optionale Verbindung zu einem bestehenden Identitätsanbieter?

Personen können auf sensible Daten ohne eine Lese- oder Schreibberechtigung zugreifen.

Sensible Daten könnten eingesehen, manipuliert oder gestohlen werden.

Vyaire SentrySuite unterstützt die Zuweisung von Benutzern zu definierten Rollen. Sie können entweder vorhandene vordefinierte Rollen verwenden, diese anpassen oder neue Rollen erstellen. Den Rollen können fein abgestufte Zugriffsrechte zugewiesen werden, so dass Sie sicherstellen können, dass Benutzer nur auf die Informationen zugreifen können, die sie für die Ausführung ihrer jeweiligen Aufgabe benötigen.

Außerdem ermöglicht SentrySuite die Zuordnung von Patientendaten zu einem Standort. Sie können z.B. Standorte für jede Ihrer Niederlassungen oder Labore anlegen. Patientendaten, die einem Standort zugewiesen sind, werden nur den Benutzern angezeigt, die an dem jeweiligen Standort arbeiten. Damit ist sichergestellt, dass Sie Patientendaten der verschiedenen Standorte trennen und die Benutzern nur Patientendaten angezeigt bekommen, die relevant für ihren Arbeitsort sind.

Welche rollenbasierte Zugriffskontrolle bietet Ihr Produkt, um sicherzustellen, dass Benutzer nur auf die Ressourcen zugreifen können, die sie benötigen? Unterstützt es verschiedene Standorte für größere Organisationen?

Updates der Anwendungs- und Gerätesoftware werden vor der Installation nicht validiert.

Angreifer können Software-Updates manipulieren, um die die Sicherheit des installierten Systems zu gefährden. Ungeschützte Geräte erleichtern Angreifern Cyberattacken - sensible Daten können eingesehen, manipuliert oder gestohlen werden.

Vyaire hat in der SentrySuite Software die Möglichkeit geschaffen, die Integrität der SentrySuite-Software-Installationsquellen und eventueller bereitgestellter Updates zu prüfen. So können Sie sicherstellen dass Installationsquellen echt sind und nicht manipuliert wurden.

Ist der Lieferant in der Lage zu prüfen, dass seine Installationsmedien sicher sind?

Geräte weden nicht mit vom Hersteller herausgegeben Sicherheitsupdates aktuell gehalten.

Ungeschützte Geräte erleichtern Angreifern Cyberattacken - sensible Daten können eingesehen, manipuliert oder gestohlen werden.

Sicherheitsupdates, die nicht vom Hersteller validiert wurden, können bei der Installation Probleme verursachen, die Ihre Geräte bis zur Behebung funktionsunfähig machen können.

Microsoft veröffentlicht kontinuierlich neue Sicherheits-Patches, um Probleme in seinen Betriebssystemen zu beheben. Neu veröffentlichte Sicherheitspatches für das Betriebssystem Windows 10 werden in der Regel innerhalb von 4 Wochen nach der Freigabe durch Microsoft von Vyaire auf Kompatibilität mit der SentrySuite Software geprüft, Die Ergebnisse dieser Kompatibilitätstests werden auf der der Vyaire Product Security Website (www.vyaire.com/product-security) zur Verfügung gestellt.

Testen Sie neue Sicherheitsupdates für Betriebssysteme auf Kompatibilität? Gibt es einen geplanten Zeitrahmen? Wie werden die Testergebnisse mit mir geteilt?

Die Geräte sind nicht gemäß empfohlener Vorgaben für maximale Sicherheit von sensiblen Daten konfiguriert.

Ungeschützte Geräte erleichtern Angreifern Cyberattacken - sensible Daten können eingesehen, manipuliert oder gestohlen werden.

Das Vyaire Produktsicherheitsteam hat zusammen mit dem SentrySuite Produktmanagement ein umfassendes SentrySuite Product Security Whitepaper erstellt. Das Whitepaper deckt alle Aspekte der Produktsicherheit ab und ermöglicht es Ihrem IT-Partner, ein professionelles Verständnis dafür zu entwickeln, wie sich SentrySuite in Ihre IT-Cybersicherheitslandschaft integrieren kann. Das Whitepaper wird für jede neue zukünftig veröffentlichte Hauptversion von SentrySuite aktualisiert.

Bieten Sie aktuelle Anleitungen zur Systemsicherheit in schriftlicher Form an?

Geräte können Ihnen oder Ihrem IT-Partner unbekannte Sicherheitslücken enthalten und damit ein zusätzliches Risiko für Ihr Netzwerk darstellen.

Ungeschützte Geräte erleichtern Angreifern Cyberattacken - sensible Daten können eingesehen, manipuliert oder gestohlen werden.

Vyaire hat sich zu einem verantwortungsvollen Offenlegungsprozess verpflichtet, um Kunden, je nach Schwere und Dringlichkeit des Problems, rechtzeitig über Sicherheitsprobleme in unseren Produkten zu informieren.

Wir veröffentlichen umfassende Informationen über potenzielle Sicherheits-bedrohungen und -probleme und informieren auf unserer Website zur Produktsicherheit (http://www.vyaire.com/product-security) darüber, was Sie tun können, um das potenzielle Risiko für Ihr Unternehmen zu verringern.

Werden Sie mich über Sicherheitsprobleme in Ihrem Produkt informieren? Wenn ja, wie und wie schnell?

Geräte können Ihnen oder Ihrem IT-Partner unbekannte Sicherheitslücken enthalten und damit ein zusätzliches Risiko für Ihr Netzwerk darstellen.

Ungeschützte Geräte erleichtern Angreifern Cyberattacken - sensible Daten können eingesehen, manipuliert oder gestohlen werden.

Vyaire führt monatliche Sicherheitsscans aller auf dem Markt unterstützen SentrySuite-Versionen durch. Vyaire verwendet branchenübliche Best Practices und Best-in-Class-Tools, um diese Scans durchzuführen. Die Scanergebnisse werden geprüft und die Behebung der gefundenen Probleme wird verfolgt und in zukünftige Softwareversionen aufgenommen.

Führen Sie regelmäßig Sicherheitsscans Ihrer Software durch (z. B. über Nessus-Scanner)? Wie oft?

Anbieter sind sich Sicherheitsproblemen in ihren Produkten möglicherweise nicht bewusst und verfügen nicht über entsprechende Ressourcen, um die Entdeckung, Verfolgung und Behebung dieser Probleme zu adressieren.

Ungeschützte Geräte erleichtern Angreifern Cyberattacken - sensible Daten können eingesehen, manipuliert oder gestohlen werden.

Vyaire hat ein Informationssicherheitsteam, das direkt an den Chief Information Security Officer berichtet. Das Team besteht aus 10 Vollzeit-Sicherheitsexperten und ist in ein Produktsicherheitsteam und ein Security Operations Center Team unterteilt.

Wie setzt sich das Team zusammen, das sich in Ihrer Organisation mit Cybersicherheit beschäftigt?

Die Geräte sind nicht gemäß empfohlener Vorgaben für maximale Sicherheit von sensiblen Daten konfiguriert.

Ungeschützte Geräte erleichtern Angreifern Cyberattacken - sensible Daten können eingesehen, manipuliert oder gestohlen werden.

Vyaire evaluiert kontinuierlich die Sicherheit von Softwarekomponenten von Drittanbietern, die bei der Entwicklung und dem Betrieb der SentrySuite-Softwarelösung eingesetzt werden. Als Teil dieser Bemühungen hat Vyaire eine konsequente Entscheidung getroffen, den Adobe Reader, der für wiederkehrende kritische Sicherheitsprobleme bekannt ist, durch eine andere, sicherere Lösung zu ersetzen, die Ihnen hilft, Ihre Gefährdung durch Sicherheitsbedrohungen zu reduzieren.

Adobe Reader ist für immer wiederkehrende Sicherheitsprobleme bekannt. Verwendet Ihr Produkt den Adobe Reader? Wenn ja, haben Sie auch sicherere Alternativen evaluiert?

Sensible Daten werden ohne geeigneten Schutz, z.B. Verschlüsselung, gespeichert.

Ungeschützte Geräte erleichtern Angreifern Cyberattacken - sensible Daten können eingesehen, manipuliert oder gestohlen werden.

Vyaire SentrySuite speichert keine sensiblen Daten (wie z. B. persönlich identifizierbare Informationen [PII] und/oder geschützte Gesundheitsinformationen [PHI]) lokal auf Benutzerarbeitsplatz-PCs.

Sensible Daten werden ausschließlich in der zentralen Datenbank gespeichert, die sich im sicheren Netzwerk-Backend in Ihrem Rechenzentrum befindet.

SentrySuite unterstützt die vollständige Verschlüsselung von Festplatten sowohl auf den Clients als auch auf dem Netzwerk-Backend-Server durch Microsoft Bitlocker. Dadurch wird sichergestellt, dass sensible Daten verschlüsselt gespeichert werden.

Speichert Ihre Lösung PHI/PII-Daten lokal, auch wenn sie mit einem Netzwerkserver verbunden ist? Wenn dies der Fall ist: Wird eine lokale Verschlüsselung der Daten (z. B. über Bitlocker) unterstützt?

Updates der Anwendungs- und Gerätesoftware werden vor der Installation nicht validiert.

Angreifer können Software-Updates manipulieren, um die Sicherheit des installierten Systems zu gefährden. Ungeschützte Geräte erleichtern Angreifern Cyberattacken - sensible Daten können eingesehen, manipuliert oder gestohlen werden.

Vyaire verwendet digitale Signaturen für alle Anwendungsdateien mit ausführbaren Code. Diese digitale Signatur hilft jedem verwendetem Antiviren- oder Anti-Malware-System die Authentizität der Anwendungsdateien festzustellen. Sie ist ein Beleg dafür, dass die signierte Datei von Vyaire Medical erstellt und verteilt wurde und echt ist.

Sind die Software-Bibliotheken Ihrer Produkte durch digitale Signaturen geschützt?

Sensible Daten werden nicht angemessen anonymisiert, bevor diese an eine dritte Partei, die keinen Zugang zu sensiblen Daten haben sollte weitergegeben werden.

Dritte können unberechtigten Zugriff auf sensible Daten erhalten.

SentrySuite ermöglicht es Ihnen, exportierte Daten zu anonymisieren, bevor Sie diese mit uns oder anderen Dritten teilen. Dies hilft Ihnen, die geltenden Datenschutzbestimmungen einzuhalten und sicherzustellen, dass die sensiblen Daten Ihrer Patienten geschützt bleiben und nicht an unbefugte Dritte weitergegeben werden.

Gibt es eine Möglichkeit, Patienten- und Messdaten auszutauschen oder im Falle einer Anfrage an die Serviceorganisation zu senden? Können diese Daten anonymisiert werden, um die Vertraulichkeit der Daten zu gewährleisten?

Verbindungen zu Informationssystemen werden nicht auf unbefugte Zugriffe aus dem Netzwerk überwacht.

Um Zugang zu sensitiven Daten zu erhalten, können Angreifer nach einem erfolgreichen Eindringen in Ihr Netzwerk unerkannt bleiben, und sich mit dem Informationssystem verbinden.

Das SentrySuite-Netzwerk-Backend überwacht kontinuierlich alle Verbindungsversuche und erkennt nicht authorisierte Verbindungsversuche. SentrySuite dokumentiert die nicht authorisierten Versuche zur weiteren Überprüfung und Analyse und liefert damit zusätzliche Informationen zu möglichen Sicherheitsproblemen in Ihrer Umgebung.

Erkennt Ihre Software unathorisierte Verbindungen? Wenn ja mit welchem System?

Sensible Daten werden ungeschützt über Ihr Netzwerk übertragen.

Angreifer können nach einem erfolgreichen Eindringen in Ihr Netzwerk leicht ungeschützte Daten während der Übertragung von System zu System abfangen. Dazu müssen die Angreifer keinen tieferen Zugriff auf Ihre Systeme erhalten.

SentrySuite unterstützt die vollständige Verschlüsselung aller Daten, die zwischen den SentrySuite-Client-Systemen und dem SentrySuite-Netzwerk-Backend übertragen werden. Die Verschlüsselung erfolgt mit Verschlüsselungsmethoden, die dem Industriestandard entsprechen, wobei die empfohlenen Vorgehensmethoden verwendet werden.

Unterstützt Ihr Produkt die Verschlüsselung von sensiblen Daten, die über mein Netzwerk übertragen werden?

## REFERENZEN


1. https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/
2. https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html
3. https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/
4. https://www.zdnet.com/article/ransomware-attacks-are-causing-more-downtime-than-ever-before/



WELTWEITER HAUPTSITZ
Vyaire Medical
26125 N. Riverwoods Blvd.
Mettawa, IL 60045
USA

Vyaire Medical GmbH
Leibnizstraße 7
97204 Höchberg
Deutschland


CE 0123



vyaire™ MEDICAL