Acronis

Cyber Protection-Lösungen für die Herausforderungen des 21. Jahrhunderts in der Gesundheitsbranche

Wie IT-Profis die sensiblen Daten im Gesundheitswesen auch im modernen Zeitalter der Cyber-Bedrohungen zuverlässig schützen können.

Die Gesundheitsbranche durchläuft einen wichtige digitalen Wandel, der weg von veralteten Methoden der Speicherung von Patientendaten und hin zu neuen, datenintensiven Diagnose- und Behandlungsanwendungen führt. Gleichzeitig unterliegen Gesundheitseinrichtungen einem enormem Druck, ihre Gewinne zu steigern, Datenschutzbestimmungen einzuhalten, die Patientenversorgung zu optimieren sowie die Interoperabilität mit Kostenträgern, Lieferanten, akademischen Einrichtungen und Patienten zu verbessern.

Die Menge an sensiblen Gesundheitsdaten wächst ständig und kann zudem über diverse physische Standorte, Computergeräte und Netzwerke (inkl. Private/Public Clouds) verteilt sein. Wichtige neue Gesundheitsanwendungen (wie Telemedizin, Fernüberwachung von Patienten oder Virtual- und Assisted-Reality-basiertes Training) tragen nicht unwesentlich zur ständig steigenden Datenflut bei. Andere aufkommende Technologien – wie künstliche Intelligenz (KI), maschinelles Lernen (ML), das Internet der Dinge (IoT) oder die Blockchain – machen das Puzzle noch komplexer. Zudem wollen immer mehr Beteiligte Zugriff auf diese Daten bekommen.

Gleichzeitig wird die Branche von einer regelrechten Flut an neuen Cyber-Bedrohungen (wie Sicherheitslücken oder Ransomware- und Kryptojacking-Angriffe) regelrecht überrollt. Es war noch nie so komplex wie heute, die Verfügbarkeit und den Schutz von Gesundheitsdaten zu gewährleisten.

Cyber-Kriminelle und feindliche staatliche Akteure haben die Gesundheitsbranche aggressiv ins Visier genommen und nutzen die Tatsache aus, dass Malware-Angriffe (z.B. mit Ransomware) besonders effektiv sind, um unberechtigten Zugriffe auf sensible, oftmals lebensentscheidende Daten zu erlangen.

Dies erklärt den rasanten Anstieg von hochkarätigen Ransomware-Angriffen auf die Gesundheitsbranche in den letzten Jahren – wovon bekannte Unternehmen und Einrichtungen wie das britische NHS (National Health Service), viele Krankenhäuser (z.B. das Hancock Health Hospital, Adams Memorial Hospital, Erie County Medical Center), die MedStar Health-Organisation und viele andere betroffen waren. Über Datenschutzverletzungen in diesem Sektor wird mittlerweile regelmäßig in den Nachricht berichtet. Dabei werden jedes Jahr Hunderte von Millionen sensibler Patienten- und Zahlungsdaten gestohlen.

Die Gesundheitsbranche befindet sich zudem im Fadenkreuz diverser Regulierungsbehörden, die auf die Einhaltung strenger Datenschutzbestimmungen pochen. Bekannte Beispiele für derartige gesetzliche Vorgaben sind die Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO/GDPR) oder HIPAA (Health Insurance Portability and Accountability Act) in den USA bzw. CCPA (California Consumer Privacy Act) in Kalifornien. Außerdem riskieren die Akteure der Branche, dass sie bei derartigen Vorfällen gegen kreditkartenrechtliche Vorgaben wie den PCI-DS-Standard (Payment Card Industry Data Security) verstoßen.

Mit der wachsenden Abhängigkeit von elektronischen Patientendaten ist auch die Wichtigkeit der permanenten Datenverfügbarkeit gestiegen. Ausfallzeiten stellen nicht nur eine offensichtliche Bedrohung der Patientensicherheit dar, sondern können so kostspielig werden, dass die Existenz einer Gesundheitseinrichtungen gefährdet ist. Laut einer Kalkulation von Gartner („Downtime Cost Calculator for Data Center Disaster Recovery Planning, 28. Februar 2014“) liegen die durchschnittlichen Kosten für die Ausfallzeiten von Unternehmen bei ca. 5.600 US-Dollar pro Minute, was etwa 300.000 US-Dollar pro Stunde entspricht. Das Unternehmen Information Technology Intelligence Consulting (ITIC) kam zu dem Schluss**, dass die geschätzten Kosten für eine Stunde Ausfallzeit für 98% aller Unternehmen rund 100.000 US-Dollar betragen. Bei großen Unternehmen können diese Kosten sogar auf 1-5 Millionen US-Dollar steigen.**

Die IT-Abteilungen von Gesundheitseinrichtungen haben mittlerweile mit denselben Herausforderungen wie andere Branchen zu kämpfen: immer komplexer werdende Infrastrukturen, Schwierigkeiten, qualifizierte Mitarbeiter zu finden und zu halten, die zunehmende Migration von Applikationen in die Cloud, vermehrte berufliche Nutzung von Mobilgeräten (Smartphones, Tablets), die Einführung neuer Monitoring- und Tracking-Systeme (IoT-Sensoren, Asset-Tracker, Webkameras etc.) sowie der Wunsch, neue Daten möglichst in Echtzeit analysieren zu können.

Um angesichts dieser Herausforderungen überleben zu können, ist ein neuer Ansatz zum Schutz und zur Sicherung von Daten erforderlich, der auf den fünf Vektoren der Cyber Protection beruht:

SAFETY (VERLÄSSLICHKEIT)

Gewährleisten, dass immer eine verlässliche Datenkopie verfügbar ist

ACCESSIBILITY (VERFÜGBARKEIT)

Ihre Daten sollten jederzeit und von überall leicht verfügbar sein

PRIVACY (VERTRAULICHKEIT)

Allein Sie sollten die volle Kontrolle über Einsicht und Zugriff auf die Unternehmensdaten haben

AUTHENTICITY (AUTHENTIZITÄT)

Weisen Sie unwiderlegbar nach, dass eine Datenkopie ein exaktes Replikat des Originals ist

SECURITY (SICHERHEIT)

Schützen Sie Ihre Daten, Applikationen und Systeme vor böswilligen Bedrohungen

Dieses Whitepaper untersucht diese grundlegenden Cyber Protection-Prinzipien anhand von sieben zentralen Herausforderungen für die Gesundheitsbranche:

1. **Die Adressierung** von Datenschutzverletzungen
2. **Der Schutz** vor Malware-Bedrohungen (wie Ransomware und Krypto-Jacking)
3. **Die Einhaltung** von Compliance-Anforderungen
4. **Die Migration** von geschäftskritischen Applikationen und Storage in die Cloud
5. **Die Bereitstellung** einer konstanten Datenverfügbarkeit
6. **Die Integration** von Mobilgeräten
7. **Die Stärkung** der Data Protection ohne dabei die Infrastruktur-Komplexität zu steigern

DIE AKTUELLE SITUATION FÜR DIE IT IM GESUNDHEITSWESEN

Datensicherung und Datensicherheit haben nach wie vor höchste Priorität im Gesundheitswesen. Das Cyber Security-Unternehmen Protenus hat in einer Studie über Datenschutzverletzungen festgestellt, dass es in 2017 mehr als einen erfolgreichen Angriff pro Tag auf Gesundheitsunternehmen gegeben hat.

Im selben Jahr kam es bei 5,6 Millionen Patientendaten zu Verstößen und es dauerte durchschnittlich 308 Tage, bis eine Einrichtung diese überhaupt feststellte.

Um diese Menge von Datenschutzverletzungen im Gesundheitswesen einzudämmen, braucht es diverse Sicherheitsebenen in der IT-Infrastruktur rund um physische Systeme, virtuelle Maschinen (VMs), Cloud Services und Mobilgeräte. Zu den grundlegenden Gegenmaßnahmen gehören ein Anti-Malware-Schutz auf allen Endpunkten, die Abwehr externer Netzwerkbedrohungen durch Firewalls sowie eine Netzwerksegmentierung über vLANs oder Software-definierte Netzwerke, um die mögliche Ausbreitung von Angriffen über das interne Netzwerk zu begrenzen. Außerdem ist eine Data Protection durch Backup- und Disaster Recovery-Funktionen unerlässlich – für den Fall, dass es einem Angriffer doch einmal gelingt, sensible Daten zu beschädigen, zu zerstören oder den Zugriff darauf zu blockieren. Dies erfordert ein zuverlässiges, verschlüsseltes Backup und dessen sichere Speicherung (möglichst on-premise und in der Cloud).

MALWARE-BEDROHUNGEN

Für die meisten Sicherheitsforscher sind die zwei gängigsten Malware-Bedrohungen der letzten Jahre, die speziell das Gesundheitswesen heimsuchen, Ransomware und Krypto-Jacker.

Ransomware infiziert Server, Desktop-PCs und Mobilgeräte im Gesundheitswesen (in der Regel durch einen Benutzer, der auf einen bösartigen Link oder Anhang in einer Phishing-E-Mail klickt), verschlüsselt alle gefundenen Daten und verlangt anschließend eine Online-Zahlung für einen Decodierungsschlüsssel, mit dem die Dateien der Opfer wieder freigegeben werden. Ohne Maßnahmen zur Erkennung und Abwehr von Ransomware-Angriffen oder die Möglichkeit zur Wiederherstellung aus einem Backup haben viele Gesundheitseinrichtungen Ausfallzeiten erlitten, die Patientenleben bedroht und Kosten in Millionenhöhe (für Produktionsausfälle und Wiederherstellungsmaßnahmen) verursacht haben.

Krypto-Jacking ist eine eher unauffälligere, aber an Bedeutung gewinnende Cyber-Angriffsart, bei der Maschinen infiziert und dann zu „Zombies" in einem Botnet gemacht werden. Ziel der Cyber-Kriminellen ist es, die Ressourcen dieser Maschinen zum digitalen „Schürfen" von Krypto-Währungen (wie Bitcoin) zu missbrauchen. Diese Art von Malware stiehlt ihren Opfern zwar „nur" Ressourcen (Rechenleistung, Arbeitsspeicher, Elektrizität, Kühlkapazitäten etc.), aber die resultierenden Energiekosten und Abnutzungsbelastungen für die Systeme können sich durchaus summieren. Hinzu kommt, dass Krypto-Mining-Malware häufig weitere Bedrohungen (wie Ransomware) in das infizierte System einschleust.

COMPLIANCE-ANFORDERUNGEN

Der Umstand, dass die Gesundheitsbranche starken regulatorischen Auflagen unterliegt, hat dazu beigetragen, dass sie zu einem bevorzugten Ziel von Malware-Angriffen geworden ist. Da die Sperrung von Patientendaten durch einen Ransomware-Angriff auch einen Compliance-Verstoß bedingt, werden die Angriffsopfer die Lösegeld-Forderung noch bereitwilliger zahlen, um ihre Daten zurückzuerhalten.

Laut dem amerikanischen „Verizon Breach Investigations Report" waren in 2019 über 70% **aller Malware-Vorfälle im Gesundheitswesen auf** Ransomware-Angriffe zurückzuführen – und das schon das zweite Jahr in Folge.

MIGRATION VON APPLIKATIONEN UND STORAGE IN DIE CLOUD

Wie viele Branchen befindet sich auch die Gesundheitsbranche in einem größeren Umbruch, bei dem Applikationen und Daten in eine Cloud-Infrastruktur (meist eine Mischung aus Public- und Private-Cloud) migriert werden sollen. Ziel dabei ist es, Kosten zu senken, komplexer abzuschreibende Kapitalaufwendungen in vorhersagbarere Betriebskosten umzuwandeln und die Verfügbarkeit der Daten von überall und mit jedem Gerät zu verbessern. Viele Institutionen kämpfen jedoch mit der Herausforderung, Storage- und Data Protection-Ressourcen sicher in die Cloud zu übertragen und dabei auch alle Datenschutz- und Compliance-Vorgaben einzuhalten.

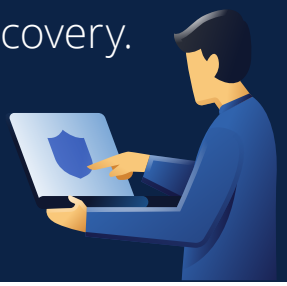
Laut dem amerikanischen „Verizon Breach Investigations Report" waren in 2019 über 70% aller Malware-Vorfälle im Gesundheitswesen auf Ransomware-Angriffe zurückzuführen – und das schon das zweite Jahr in Folge.

DATENVERFÜGBARKEIT

Die Gesundheitsbranche legt aus offensichtlichen Gründen viel Wert auf eine hohe und kontinuierliche Datenverfügbarkeit: nicht nur die Gesundheit, sondern sogar das Überleben der Patienten kann davon abhängen.

In Bezug auf Backup und Recovery bedeutet dies, dass IT-Profis im Gesundheitswesen besonders auf zwei Messgrößen achten müssen: die Wiederherstellungspunktvorgabe (kurz RPO, für Recovery Point Objective) und die Wiederherstellungszeitvorgabe (kurz RTO, für Recovery Time Objective). Der RPO-Wert definiert, wie viele Datenverluste ein Unternehmen zu einem bestimmten Zeitpunkt hinnehmen kann/möchte: was mit anderen Worten bedeutet, in welchen Zeitabständen die Daten durch Backups gesichert werden müssen. Der RTO-Wert entspricht der maximalen Ausfallzeit, die zwischen einem Datenausfallereignis und der anschließenden erfolgreichen Wiederherstellung tolerierbar ist. Die meisten Institutionen können leicht ermitteln, welche Applikationen strenge RPOs und RTOs erfordern – und welche einen höheren Datenverlust und längere Wiederherstellungszeiten verkraften können.

Acronis bietet Gesundheitseinrichtungen ein komplettes Set von anwenderfreundlichen, extrem flexiblen und stark integrierten Lösungen für Cyber Protection, Storage und Disaster Recovery.



BYOD-RISIKEN

BYOD (Bring Your Own Device) beschreibt den Trend, dass Angestellte ihre eigenen Geräte (v.a. die allgegenwärtigen Mobilgeräte) auch für die Arbeit verwenden wollen. Für Unternehmen kann dies Vorteile bringen, wie etwa bessere Produktivität und Zusammenarbeit der Mitarbeiter. Es ist aber auch eine Herausforderung für den Datenschutz, weil damit vertrauliche Daten häufiger auf Geräten gespeichert werden, die leicht gehackt, gestohlen oder verloren gehen können.

VEREINFACHTE CYBER PROTECTION

Auch die IT-Manager der Gesundheitsbranche kämpfen mit Fachkräftemangel. Die betriebliche Komplexität zu verringern, ist daher zu einer der wichtigsten Prioritäten geworden. Dies gilt insbesondere für IT-Routineaufgaben wie Data Protection-Maßnahmen. Es ist beispielsweise suboptimal, viele Systeme bereitstellen zu müssen, um ein heterogene IT-Umgebung zu verwalten – und dafür auch noch hochqualifizierte Experten zu benötigen.

ACRONIS CYBER PROTECTION-LÖSUNGEN FÜR DAS GESUNDHEITSWESEN

Acronis kann Unternehmen auf mehreren Ebenen vor Datenschutzverletzungen bewahren. Acronis Cyber Backup beispielsweise gewährleistet durch eine zuverlässige Datenverschlüsselung (bei Speicherung und Übertragung), dass Cyber-Kriminelle – selbst im Falle eines erfolgreichen Datenverstoßes – nicht von den Informationen profitieren können, die sie vermeintlich kompromittiert haben.

Außerdem können mit Acronis Cyber Backup alle Daten, die bei einem Cyber-Angriff manipuliert, zerstört oder gesperrt wurden, vollständig wiederhergestellt werden.

Acronis Cyber Cloud Storage kann Ihre Daten und Backups durch ein beeindruckendes Spektrum an Cyber-Abwehrmaßnahmen (inkl. der starken Datenverschlüsselung) und der Speicherung in unseren zertifizierten Cloud-Datenzentren zuverlässig schützen.

DER SCHUTZ VOR MALWARE-BEDROHUNGEN (WIE RANSOMWARE UND KRYPTO-JACKING)

Acronis Cyber Backup mit integrierter Acronis Active Protection-Technologie verwendet künstliche Intelligenz (KI) und maschinelles Lernen (ML), um verdächtige Änderungen an Daten, Backup-Dateien und Backup-Agenten proaktiv zu erkennen, zu blockieren und zu beseitigen. Nicht autorisierte Dateiänderungen können über einen speziellen Zwischenspeicher (Cache) oder aus Backups zurückgesetzt werden. Auch Krypto-Jacking-Angriffe werden automatisch erkannt und gestoppt.

Dies ermöglicht eine außergewöhnliche Abwehr der zwei gängigsten Malware-Bedrohungen im Gesundheitswesen – und ergänzt herkömmliche Abwehrmaßnahmen (wie signaturbasierte Antiviren-Software) um einen Schutz vor Zero-Day-Bedrohungen.

Acronis Cyber Backup sichert außerdem seinen Backup Agenten und seine Backup-Archive gegen Malware-Angriffe ab. Dadurch wird gewährleistet, dass ein Unternehmen seine Daten und Systeme nach einer Sicherheitsverletzung schnell wiederherstellen und den normalen Geschäftsbetrieb wieder aufnehmen kann.

DIE EINHALTUNG VON COMPLIANCE-ANFORDERUNGEN

Mit ihren Verschlüsselungsfähigkeiten unterstützen Acronis Cyber Backup mit Acronis Active Protection und Acronis Cyber Cloud Storage ebenfalls die Einhaltung von Compliance-Zielen, indem Sie die Vertraulichkeit von sensiblen Gesundheitsdaten gewährleisten. Selbst wenn Cyber-Kriminellen ein Einbruch gelingt, sind die erbeuteten Daten für sie nutzlos. Acronis Produkte verfügen über eine Vielzahl weiterer Funktionen und Merkmale, die – sofern richtig konfiguriert und eingesetzt – die Einhaltung gesetzlicher Vorgaben wie HIPAA und HITECH (US-Datenschutzvorschriften für das Gesundheitswesen) ermöglichen. Obwohl es kein offizielles, rechtlich anerkanntes Zertifizierungs- oder Akkreditierungsverfahren für HIPAA oder HITECH gibt, **betreibt Acronis ein spezielles Sicherheits- und Compliance-Programm, um mögliche Bedenken seiner Kunden bezüglich der Einhaltung von HIPAA und HITECH zu minimieren.** Weitere Informationen finden Sie im Acronis Resource Center.

DIE MIGRATION VON GESCHÄFTSKRITISCHEN APPLIKATIONEN UND STORAGE IN DIE CLOUD

Acronis Cyber Backup vereinfacht die Migration von Applikationen in die Cloud, indem es eine breite Palette von Cloud Services, Betriebssystemen (physisch und virtuell), Applikations-Workloads (lokal und Cloud-basiert) sowie Endgeräten unterstützt. Durch die umfangreichen Daten-Management-Tools von Acronis Cyber Backup können Workloads einfach und sicher zwischen unterschiedlichen Umgebungen verschoben werden. Dies ermöglicht schnelle, gefahrlose Migrationen zwischen physischen und virtuellen Umgebungen, Private Clouds, dem Acronis Cyber Cloud Storage oder den beliebten Public Cloud-Angeboten von Amazon, Google oder Microsoft.

DIE BEREITSTELLUNG EINER KONSTANTEN DATENVERFÜGBARKEIT

Acronis Cyber Backup bietet nützliche Funktionen, die Gesundheitseinrichtungen bei der intelligenten Verwaltung von RTOs und RPOs in ihrer Umgebung unterstützen. Zu diesen Funktionen gehören:

1. Acronis Instant Restore – ermöglicht kürzeste RTO- und RPO-Werte und damit auf wenige Sekunden reduzierte Ausfallzeiten für unternehmenskritische Applikationen
2. Acronis Universal Restore – stellen Sie Ihre Systeme flexibel auch auf abweichender/fabrikneuer Hardware oder einer anderen Plattform (z.B. physische auf virtuellen Maschinen) wieder her
3. Acronis Active Protection – diese in allen Produkten integrierte Technologie verhindert Ausfälle und Leistungseinbußen durch Ransomware- und Krypto-Jacking-Angriffe.

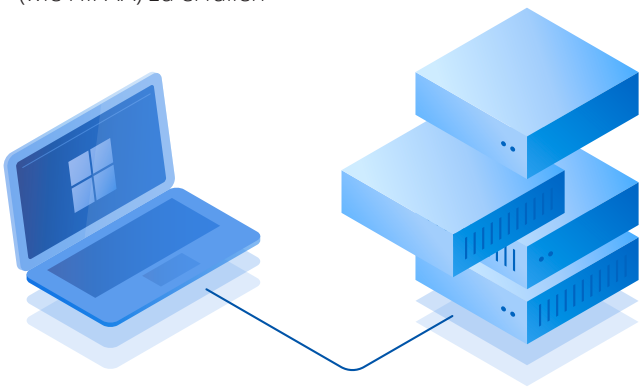
DER SCHUTZ VON SENSIBLEN DATEN AUF ALLEN GERÄTEN

Acronis Files Advanced hilft, die Patientenversorgung und betriebliche Effizienz zu verbessern, und gewährleistet dabei die Einhaltung strenger Sicherheits- und Compliance-Standards (wie der US-Datenschutzverordnung HIPAA). Mit Acronis Files Advanced können Mitarbeiter, Partner und Auftragnehmer sensible Gesundheitsdaten sicher austauschen oder gemeinsam bearbeiten. Die jeweiligen Unternehmen behalten dabei die vollständige Kontrolle über die Speicherung, Verwaltung und Vertraulichkeit ihrer Daten.

Die Acronis Files Advanced Policy Engine bietet granulare Data Management-Funktionen, um Inhalte, Benutzer und Geräte genau kontrollieren und die Einhaltung von Compliance-Auflagen sicherstellen zu können. Unsere Lösung garantiert durch eine sichere Ende-zu-Ende-Verschlüsselung (bei Speicherung und Übertragung) die vollständige Sicherheit und Vertraulichkeit aller verwendeten Daten. Mit Acronis Files Advanced können IT-Abteilungen Sicherheitsverletzungen (wie Informationslecks und verbotene Datenfreigaben) über zentrale Richtlinienkontrollen effizient unterbinden.

Gesundheitsdienstleister, Arztpraxen und Patienten verwenden Acronis Files Advanced, um auf Gesundheitsdaten zuzugreifen, diese zu bearbeiten, zu erstellen oder zu teilen – und das mit jedem Gerät (Desktop-PCs, Laptops, Tablets oder Smartphones). Arztpraxen und andere Medizineinrichtungen nutzen die Lösung außerdem:

- um sensible Patientendaten und Verwaltungsdokumente zu schützen (z.B. vertrauliche Informationen, Forschungsunterlagen, Verträge etc.).
- **um Ärzten,** Forschern und Administratoren einen sicheren Zugriff auf Gesundheitsdaten zu ermöglichen und diese von jedem Gerät aus leicht freigeben zu können
- **Patientendaten bei** Übertragung und Speicherung abzusichern
- **damit interne Mitarbeiter untereinander** und mit externen Partnern schnell und effizient bei der Patientenversorgung zusammenarbeiten können
- **um Zugriffe** auf und Freigaben von medizinischen Dateien zu überwachen
- **um strenge** Sicherheits- und Compliance-Standards (wie HIPAA) zu erfüllen



MEHR CYBER PROTECTION OHNE DIE INFRASTRUKTUR-KOMPLEXITÄT ZU ERHÖHEN

Mit Acronis Cyber Backup wird die Umsetzung von Cyber Protection-Anforderungen im Gesundheitswesen einfacher und kostengünstiger. Denn es kann über eine einzige, integrierte Plattform alle Workloads eines Unternehmens effizient schützen.

Es kann Storage-, Aufbewahrungs-, Backup- und Recovery-Operationen zentral und Plattform-übergreifend verwalten. Dabei werden marktübliche physische, virtuelle, mobile und Cloud-Plattformen genauso unterstützt, wie gängige Workloads von Microsoft, Oracle, Google und anderen Anbietern. Die intuitive, leistungsfähige Benutzeroberfläche mit ihren zahlreichen Monitoring-Tools ist auch für weniger erfahrene IT-Mitarbeiter leicht zu bedienen. Daher können sich die erfahrenen IT-Mitarbeiter auf strategisch wichtigere Projekte konzentrieren.

Und schließlich gibt es noch das Acronis Disaster Recovery Add-On – eine einfache, anwenderfreundliche Erweiterung für Acronis Cyber Backup. Damit können Gesundheitseinrichtungen ihre geschäftskritischen IT-Systeme, Applikationen und Daten bei einem Vorfall/Ausfall umgehend wiederherstellen. Dazu werden die Systeme automatisch auf virtuelle Maschinen umgeschaltet, die aus zuvor erstellten Backups heraus in der sicheren Acronis Cloud ausgeführt werden. Das Add-on bietet Failover-Fähigkeiten für eine Vielzahl gängiger Plattformen und Applikationen – wie etwa Windows- und Linux-Server, diverse Virtualisierungsplattformen (VMware, Hyper-V, KVM, XenServer, Red Hat Virtualization u.a.) sowie Microsoft-Applikationen (wie Exchange, SQL Server, SharePoint und Active Directory).

DIE EINZIGARTIGE ACRONIS CLOUD-ARCHITEKTUR GIBT IHNEN DIE KONTROLLE ÜBER IHRE DATEN

FREIE WAHL DER VERWALTUNG

Management-Software wird unabhängig bereitgestellt und kontrolliert – für volle Kontrolle über die Data Protection durch Kunden, Service Provider, Hersteller, Partner oder Drittanbieter über Public/Partner/Private Cloud oder lokal beim Kunden

BELIEBIGE DATA PROTECTION

- Backup
- Storage
- Disaster Recovery
- Synchronisierung und Freigabe
- Notary/ASign
- Ransomware-Schutz

BELIEBIGE WORKLOADS

- Lokal
- Private Cloud
- Cloud
- Mobilgeräte
- Applikationen
- Dateien
- Virtuell

BELIEBIGER STORAGE

- Laufwerk, Band
- NAS, SAN
- Partner-Cloud
- Private Cloud
- Public Cloud
- Acronis Cloud

BELIEBIGE BEREITSTELLUNG

- Lokal
- Private Cloud
- Partner-Cloud
- Acronis Cloud
- Public Cloud

BELIEBIGES RECOVERY

- Physisch
- Virtuell
- Mobilgeräte
- Applikationen
- Dateien
- Cloud

FAZIT

Der schnelle digitale Wandel, steigende Datenmengen, wachsende Anforderungen an die Interoperabilität und eine zunehmende Kontrolle durch Anteilseigner und Regulierungsbehörden bewirken alle zusammen, dass die Gesundheitsbranche derzeit vor ganz besonderen Herausforderungen steht. Es ist eine schwierige Angelegenheit, einen Ausgleich zwischen den unterschiedlichen Anforderungen für Verlässlichkeit, Verfügbarkeit, Vertraulichkeit, Authentizität und Sicherheit zu finden. Insbesondere wenn man sich Armeen von Cyber-Kriminellen gegenübersieht, die entschlossen versuchen, wertvolle Gesundheitsdaten zu stehlen und dafür Lösegeld zu erpressen. Von Einrichtungen im Gesundheitswesens wird erwartet, komplexe neue Anwendungen zu ermöglichen, Kosten zu senken und die Patientenversorgung zu verbessern. Und dabei sollen gleichzeitig noch umfassende IT-Herausforderungen – wie hohe Personalbindung, fortschreitende Cloud-Migration und zunehmende Nutzung von IoT- und Mobilgeräten – bewältigt werden.

Acronis kann bei der Bewältigung dieser Aufgaben und Herausforderungen helfen, weil es eine bewährte Reihe von Cyber Protection-, Storage-, File Sync & Share- und Disaster Recovery-Lösungen anbietet, die optimal für die Gesundheitsbranche geeignet sind.

Lesen Sie wie ein US-Krankenhaus bereits von den Acronis Cyber Protection-Lösungen profitieren konnte.

Sie können hier kostenlose **30-tägige Testversionen von Acronis Produkten** für die Gesundheitsbranche anfordern:

- Acronis Cyber Backup mit Acronis Active Protection — KOSTENLOSE 30-TÄGIGE TESTVERSION ANFORDERN
- Acronis Disaster Recovery Add-On für Acronis Cyber Backup — KOSTENLOSE 30-TÄGIGE TESTVERSION ANFORDERN
- Acronis Files Advanced — KOSTENLOSE 30-TÄGIGE TESTVERSION ANFORDERN

Acronis

Weitere Informationen erhalten Sie unter **www.acronis.com**