Weniger Risiken. Mehr Effizienz. Und eine bessere Patientenversorgung durch moderne Datensicherung.

Effizienzsteigerung, optimierte Prozesse und Kostendruck sind die Treiber für die Digitalisierung des Gesundheitswesens. Eine vorausschauende Diagnostik, neue Therapien und eine bessere Überwachung und Betreuung von Patienten erfordern aber vor allem die Erhebung und Speicherung hochsensibler Daten, die in einem Umfeld, das vermehrt Angriffen von außen ausgesetzt ist, besonders geschützt werden müssen. Für den Schutz dieser kritischen Systeme gibt es intelligente Backup- und Recovery-Lösungen, die gleich mehrere Herausforderungen im Gesundheitswesen lösen können.

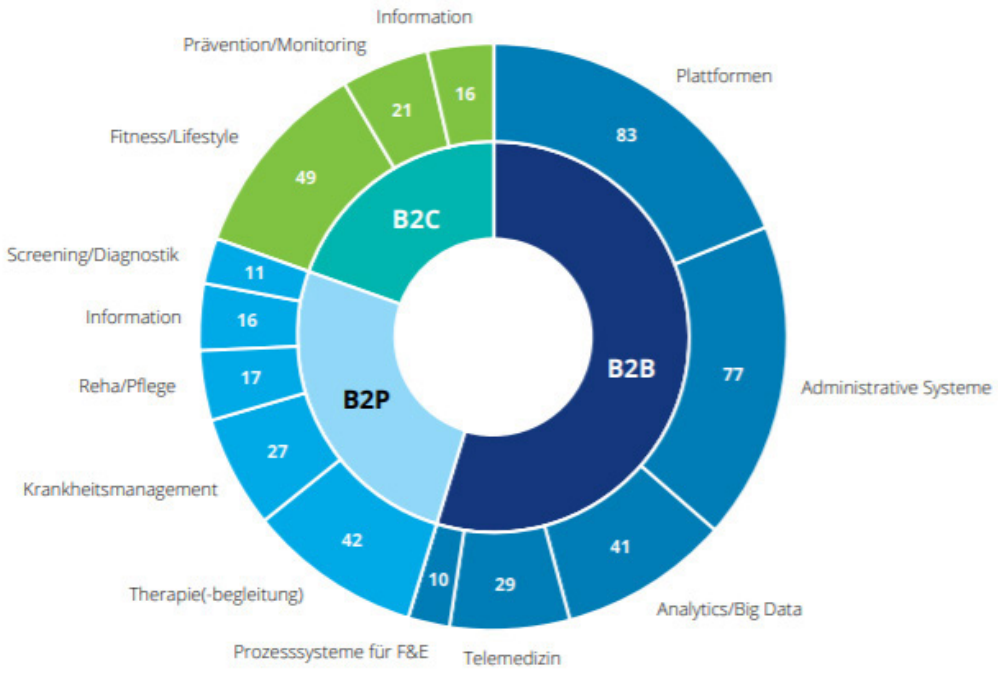
Inhaltsverzeichnis

Die Digitalisierung des Gesundheitswesens – Chancen und Herausforderungen

Die digitale Transformation schreitet in allen Bereichen der Gesellschaft immer weiter voran. Unternehmen aller Wirtschaftsbereiche versprechen sich von der Digitalisierung schnellere, transparentere Prozesse, eine erhöhte Agilität und punktuelle Kosteneinsparungen durch die Entzerrung und Entlastung der eigenen IT-Infrastruktur. Die gleichen Treiber sorgen auch bei Unternehmen des Gesundheitswesens für eine beschleunigte Digitalisierung.

Das zeigt nicht zuletzt die immer weitere Verbreitung von digitalen Endgeräten wie Smartphones, Computer und Tablets im Gesundheitsbereich, aber vor allem auch die größere Verfügbarkeit von speziellen Software-/App-Anwendungen, die vermehrt in diesem Sektor zum Einsatz kommen. Neben übergreifenden Gerätekategorien wie Smartphones existierten im Jahr 2016 In Deutschland knapp 11 Millionen digitale Endgeräte speziell im und für den Gesundheitsbereich.[1]

Abb. 1 – Übersicht digitaler Gesundheitsangebote in Deutschland (basierend auf Stichprobe)



Angaben in absoluten Zahlen

Hinweis: n=439 Kategorisierungen der Angebote von 270 Anbietern
Quellen: Angel.co, Crunchbase, Deloitte-Analyse

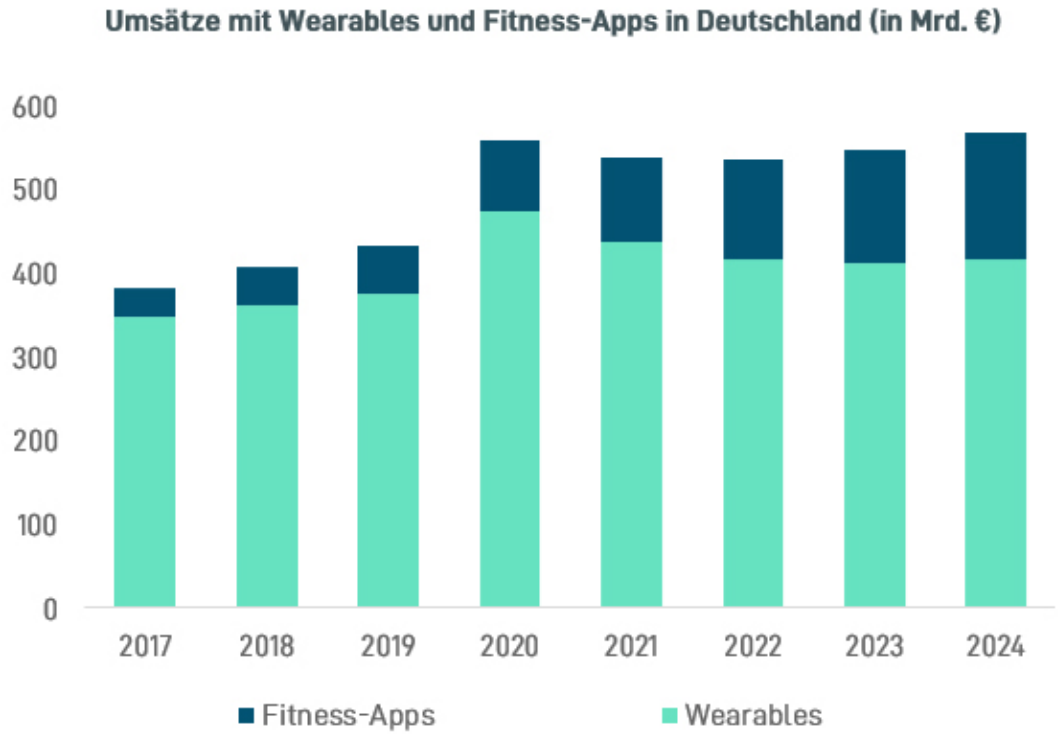
[1] Digitalisierung des Gesundheitsmarktes, Studie 2021, Deloitte

Vitalparameter als weiterer Treiber der Digitalisierung

Die Attraktivität und Funktionsumfänge von Sensoren, die früher nur in Großgeräten zum Einsatz kamen, und jetzt in sogenannten „Wearables" unmittelbar am Patienten getragen Vitaldaten direkt an die Systeme zur

Überwachung übertragen, sind ein weiterer wichtiger Treiber für die digitale Transformation im Gesundheitsbereich.

Und die technologische Entwicklung geht hier noch weiter. Laut einer Studie über die „Digitalisierung des Gesundheitsmarktes" könnte sich dieser Trend durch implantierbare Mikro-Sensoren fortsetzen. Die Möglichkeiten, die sich dadurch eröffnen, sind vielversprechend. Durch die Speicherung und Nutzung der von diesen Endgräten erhobenen Daten verspricht man sich Vorteile vor allem für eine zielgerichtete Diagnostik, auf deren Basis sich neue, individuelle Therapien entwickeln lassen. Außerdem könnten so klinische Entscheidungen analytisch fundiert unterstützt werden.



Es geht immer auch um Kostensenkung

Marktteilnehmer des Gesundheitswesens wie Regulatoren, Patienten, Kostenträger und Leistungserbringer, erhoffen sich von der Digitalisierung jedoch nicht nur den schnelleren Zugang zu und flexibleren Umgang mit Gesundheitsdaten, sondern vor allem mehr Effizienz in den Abläufen im Gesundheitssektor. Denn mehr Effizienz senkt die Kosten, und der Kostendruck ist gerade im Gesundheitssektor immens. In einer Studie geht man davon aus, dass sich im Jahr 2018 bis zu 38 Mrd. Euro Verbesserungspotenzial hätten realisieren lassen, wenn das deutsche Gesundheitswesen bereits digitalisiert arbeiten würde, was rund 12 % des tatsächlichen Gesamtaufwands von hochgerechnet etwa 290 Mrd. Euro in 2018 ausmacht.[2]

Zwei Beispiele: Die o. g. Überwachung von Vitalparametern (eICU) wurde in der McKinsey Studie als eine von 26 digitalen Gesundheitstechnologien der Lösungskategorie „Arbeitsabläufe/Automatisierung" zugeordnet. Zu dieser Kategorie gehören u. a. noch die mobile Vernetzung des Pflegepersonals, die barcodebasierte Verabreichung von Medikamenten oder RFID-Tracking. In diesem Bereich ließen sich insgesamt 6,1 Mrd. Euro einsparen.

Mit insgesamt 9 Mrd. Euro hat die Lösungskategorie „Papierlose Daten" laut dieser Studie das weitaus größte Einsparpotential. Allein 6,4 Mrd. Euro ließen sich demnach in diesem Bereich einsparen, wenn man im Gesundheitswesen eine einheitliche elektronische Patientenakte einführen würde.

[2] Digitalisierung im Gesundheitswesen: Chancen für Deutschland, Studie 2018, McKinsey

Der Schutz von Daten in „Kritischen Infrastrukturen“

Kurz: Effizienzsteigerung, optimierte Prozesse und Kostendruck treiben Unternehmen des Gesundheitssektors an, zu digitalisieren. Und ganz gleich, von welcher Seite man dieses Bestreben betrachtet oder welche Bereiche zuerst digitalisiert werden können: In jedem Fall fallen hochsensible Daten an, die verwaltet, kontrolliert, geschützt und gesichert werden müssen. Das ist zwar in Unternehmen anderer Branchen nicht anders, aber im Gesundheitswesen geht es vorwiegend um sogenannte kritische Infrastrukturen. Systeme, die eine Fülle an hochsensiblen Patientendaten speichern und zur Verfügung stellen. Daten, die Diagnosen und Therapien beeinflussen und zu jederzeit zur Verfügung stehen müssen – in Krankenhäusern sogar in Echtzeit während eines Eingriffes oder einer Behandlung. Ein Ausfall der Systeme vor allem durch Cyber-Attacken kann demnach verheerende Folgen für die Gesundheit eines Menschen haben. Daten in solchen kritischen Systemen müssen deshalb ganz besonders geschützt werden – ganz gleich ob sie in der Cloud oder physischen Systemen direkt vor Ort vorgehalten werden.

Ein dramatischer Anstieg von Cyber-Attacken

Cybersicherheitsvorfälle stellen für Unternehmen das größte Geschäftsrisiko dar.[3] Und das gilt auch für Unternehmen der Gesundheitsbranche, insbesondere Krankenhäuser.

Allein in den letzten zwei Monaten im Jahr 2020 sind die Cyber-Angriffe auf deutsche Krankenhäuser um 220 % gestiegen.[4] Bei einem IT-Sicherheitscheck von vernetzten Medizingeräten wie z. B. Insulinpumpen oder Herzschrittmachern, wurden allein 150 Schwachstellen identifiziert, die von Hackern genutzt werden könnten.[5] Das hat nicht zuletzt dazu geführt, das IT-Sicherheit in den Management-Etagen der Krankenhäuser zum Top-Thema geworden ist. Es geht darum, wie man die Themen IT-Sicherheit, effiziente Arbeitsabläufe und bessere Behandlungen in einen machbaren Einklang bringen kann. In den Vorstandsetagen geht man grundsätzlich davon aus, dass Kliniken bei der Einhaltung von Compliance-Vorschriften und Sicherheitsvorgaben besser aufgestellt sind als Unternehmen anderer Branchen. Auch die Dringlichkeit von Cybersicherheit wird hier durchaus verstanden, ein Umstand, der durch die Vorfälle in großen Kliniken durch Ransomware-Angriffe noch verstärkt wird. Eine trügerische Sicherheit, die vor allem auch kleinere und mittelgroße Kliniken betrifft. Denn obwohl immer mehr Geld in die IT-Sicherheit investiert wird, steigt die Anzahl der Cybersicherheitsvorfälle seit geraumer Zeit immer mehr an.[6] Und das wird genau dann zum Problem, wenn etablierte Fähigkeiten und herkömmliche Methoden nicht mehr ausreichenden Schutz bieten und insgesamt nicht flexibel genug sind, um Cybersicherheitsvorfälle rechtzeitig zu erkennen und vorzubeugen. Sind sie erstmal eingetreten, ist es zu spät. Dann geht es nur noch darum, Datenverluste zu vermeiden und verlorengegangene Daten einfach wiederherzustellen. Doch das scheint aktuell noch ein Problem zu sein. Eine von Veeam in 2021 veröffentlichte Studie[7] ergab, dass **78 %** der Gesundheitsorganisationen eine Verfügbarkeitslücke von Daten haben und knapp die Hälfte also **47 %** verlorengegangener Daten nicht wieder hergestellt werden können. Hier besteht allzu deutlicher Handlungsbedarf.

[3] Allianz Risk Barometer, 2020

[4] Check Point Research, 2021

[5] Manipulation von Medizingeräten, 2020, BSI, aus Medical Tribune

[6] Security Outcomes Study, Healthcare Sector, 2021, Cisco

[7] Data Protection Report, Veeam, 2021

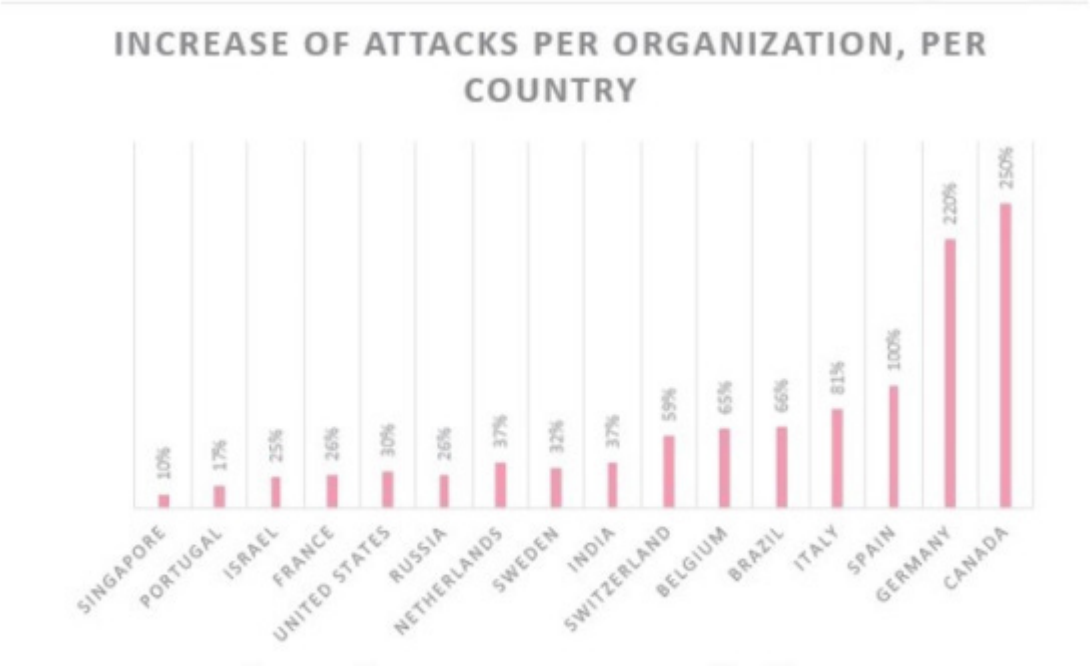


Abbildung 1: Anstieg der Attacken im Gesundheitsbereich nach Ländern

Wer es macht, oder: Das Ressourcen-Problem der Branche

Gerade bei Letztgenannten tritt dann auch ein weiteres Problem auf: der Mangel an IT-Security-Spezialisten, ein echtes Ressourcen-Problem. Das liegt teilweise auch daran, dass andere Branchen oft attraktiver sind, ein Umstand, der sich nicht einfach lösen lässt. Doch hier wird deutlich, wie wichtig effiziente Abläufe und Technologien sind, die unternehmensweit unerwünschte Vorfälle zeitnah erkennen und entschärfen können. Und die bei Eintritt eines unvorhergesehenen Schadens Datenverluste verhindern und kritische Daten gegebenenfalls in Echtzeit wiederherstellen können, ohne die IT-Abteilung im Alltagsbetrieb zusätzlich unnötig zu belasten. Der Nutzerperspektive kommt demnach bei der Sicherung von Gesundheitsdaten eine erhöhte Bedeutung zu. Es geht darum, durch die Automatisierung von Warnungen und Berichten über Cyber-Bedrohungen in Gesundheitseinrichtungen Zeit und Kapazität der Mitarbeiter zu sparen. Die Antwort auf dieses Ressourcen-Problem ist Backup- und Recovery-Lösungen, die einfach zu bedienen sind und einen Self-Service von Anwendungen und Plattformen bieten.

Noch mehr Kostendruck durch hohe gesetzliche Anforderungen

Die gesetzlichen Anforderungen für den Schutz kritischer Infrastrukturen (Kritische Systeme) sind hoch und setzen Gesundheitseinrichtungen zusätzlich unter Kostendruck. Das Monitoring von Gesundheitsdatensicherungen zur Früherkennung von Sicherheitsverletzungen durch Cyber-Angriffe ist dabei ein wichtiger Bestandteil, um die gesetzlich vorgeschriebenen Schutzmaßnahmen der kritischen Infrastrukturen im Gesundheitswesen transparent zu machen. Tritt ein Schadensfall ein, ist der Halter der sensiblen Daten dafür verantwortlich, nachzuweisen, dass er ausreichende Vorkehrungen für ein vorschriftsmäßiges Backup und effiziente Methoden zur schnellen Wiederherstellung der Daten nicht nur getroffen hat, sondern auch dokumentiert nachweisen kann.

Es geht um die lückenlose Rückverfolgbarkeit von Schutzmaßnahmen – ein wesentlicher Baustein für den Aufbau eines kontinuierlichen Cyber-Risikomanagements. Einem Backup- und Recovery-System, das umfangreiche Management- und Analyse-Funktionen bietet, kommt damit bei der Einhaltung der gesetzlichen Vorschriften eine erhöhte Bedeutung zu.

Eine Schlüsselrolle für Backup- und Recovery-Systeme

Backup- und Recovery-Lösungen sind nicht neu. Und sie sind kein reines Cloud-Thema. Denn überall, wo Daten gespeichert werden, sorgen solche Systeme dafür, dass bei Sicherheitsvorfällen jeglicher Art – ganz gleich, ob sie durch menschliches Versagen, IT-interne Störungen oder Angriffe von außen entstanden sind – sichergestellt wird, dass Datenverluste vermieden und Daten auf einen beliebigen Stand wiederhergestellt werden können. Die Bedeutung dieser Systeme ist aber durch die digitale Transformation von Unternehmen wesentlich größer geworden. Mit den notwendigen Funktionen ausgestattet, sorgen Backup- und Recovery-Systeme gerade im Gesundheitswesen dafür, dass die Anforderungen, die sich im Rahmen einer Business Continuity, im Ressourcen-Management, durch Kostendruck und durch gesetzliche Bestimmungen stellen, vollumfänglich erfüllt werden können.

Geschäftskontinuität, oder: Warum schnell nicht gleich schnell ist

Im Wesentlichen geht es darum, dass bei Eintritt eines wie auch immer gearteten Schadensfalles Daten aus einem Backup-System schnell wiederhergestellt werden können, damit ein Unternehmen störungsfrei weiterarbeiten kann. Aber was ist schnell? Ein Beispiel: Ein Industrieunternehmen hat durch den Ausfall seines ERP-Servers keinen Zugriff auf seine Kunden- und Finanzdaten. Das Recovery der Daten und Aufspielen auf einen Ersatzserver dauert eine knappe Stunde – und ist nicht lebensbedrohlich. Bei einem IT-Ausfall durch einen Cyber-Angriff, bei dem das medizinische Personal wichtige Patientendaten während einer Operation oder Behandlung benötigt, ist eine Stunde indiskutabel und kann überdies für den Patienten lebensgefährlich sein. Geschäftskontinuität ist also nicht überall gleich einzuschätzen, in Unternehmen der Gesundheitsbranche hat sie allerdings oberste Priorität.

Fazit: Ein modernes Backup- und Recovery-System muss in der Lage sein, Daten nicht nur vor Cyber-Angriffen wie Ransomware allumfänglich zu schützen, sondern muss Produktivdaten sofort und in Echtzeit wieder zur Verfügung stellen können.

Ressourcen-Management und Kostendruck, oder: Warum einfach so vieles einfacher macht

Dass Unternehmen aus dem Gesundheitssektor unter Personalmangel leiden, ist bekannt. Das betrifft allerdings nicht nur das Pflegepersonal, sondern auch die IT-Mitarbeiter. Weil die IT-Abteilung in der Regel mit den Alltagsaufgaben ausgelastet ist, Cyber-Angriffe aber dramatisch zugenommen haben, gilt es, für Schutz-Lösungen zu sorgen, die Cyber-Bedrohungen frühzeitig erkennen, abwehren und eine etwaige Wiederherstellung von Daten so einfach und einfach wie möglich machen. Und weil – nicht zuletzt durch die Privatisierung – auch der Kostendruck in diesen Unternehmen enorm hoch ist, muss Backup und Recovery so kostengünstig wie möglich realisiert werden können.

Fazit: Ein modernes Backup- und Recovery-System muss eine moderne und intelligente Wiederherstellung bieten, die einfach zu bedienen ist, Backups mit Self-Service erlaubt und dabei umfangreiche Reports und Analyse-Funktionen bietet, um zukünftigen Bedrohungen vorbeugen zu können. Das Lizenzmodell sollte so transparent sein, dass die Berechnung und eine Planung der Ressourcen wesentlich vereinfacht wird.

Gesetzliche Anforderungen, oder: Wer schreibt, der bleibt

Einige der wichtigsten Anforderungen, die Unternehmen im Gesundheitswesen erfüllen müssen, sind vom Gesetzgeber vorgegeben. Dazu gehört, dass Unternehmen nachweisen müssen, dass sie Daten gemäß den gesetzlichen Bestimmungen schützen. Wer diese Anforderungen nicht erfüllt, muss mit rechtlichen Sanktionen oder empfindlichen Geldbußen rechnen, verliert aber dazu noch seine Reputation. Organisatorisch ist das aufwendig, vor allem, wenn es darum geht, auch zu dokumentieren, wie man sich gegen Cyber-Attacken schützt oder wie man verlorengegangene Daten sicher und schnell wiederherstellt.

Fazit: Ein modernes Backup- und Recovery-System muss ein detailliertes Reporting bei Cyber-Angriffen automatisiert zur Verfügung stellen können und die Möglichkeit bieten, die Wiederherstellung von Daten für Dritte nachvollziehbar dokumentieren zu können.

Veeam® Availability Suite™ – Eine Lösung für alle Anforderungen

Die Komplett-Lösung für Sicherung, Wiederherstellung und Monitoring von Patientendaten

Die Veeam® Availability Suite™ (VAS) vereint die Monitoring-Funktionalitäten von Veeam ONE™ und die leistungsstarken Datensicherungs-Features von Veeam Backup & Replication™ in einer Enterprise-Komplettlösung für alle Anforderungen in Sachen Datensicherung und Analyse für den Gesundheitssektor.

Die Kombination dieser zwei branchenführenden Produkte genügt höchsten Datensicherungsansprüchen und liefert gleichzeitig detaillierte Einblicke in die Konfiguration, sodass sich Gesundheitsdaten noch besser schützen, Ressourcen besser planen, Kosten senken und gesetzliche Bestimmungen erfüllen lassen.

Leistungsüberblick:

- VAS bietet einen zuverlässigen, erweiterbaren Ansatz für cloudbasierte Sicherung und Wiederherstellung von Daten.
- Potenzielle Bedrohungen lassen sich durch proaktive Benachrichtigungen entschärfen, bevor sie zu Problemen werden.
- Mit den integrierten intelligenten Automatisierungs- und Diagnose-Tools lassen sich Kosten für die Behebung häufiger Infrastruktur- und Backup-Probleme senken und Reaktionszeiten erheblich verkürzen.
- Rund um die Uhr immer auf dem aktuellen Informationsstand mit Echtzeiteinblick in physische, virtuelle und Backup-Umgebungen.
- VAS liefert verlässliche Zahlen, um den zukünftigen Infrastrukturbedarf zu prognostizieren und Storage-Investitionen besser zu planen.
- Risikominimierung durch Einhaltung von Governance und Compliance, wodurch Daten stets sicher und vor Angriffen wie z. B. durch Ransomware geschützt sind.
- Die Berechnung der Ressourcen- und Storage-Kosten pro Benutzer/Gruppen spart Zeit und vereinfacht die Planung.

Kurz: Veeam bietet mit seiner ausgewiesenen Expertise und seinem umfangreichen Partnernetzwerk mit der Veeam® Availability Suite™ die Komplettlösung für eine moderne Datensicherung unabhängig von Anwendungen oder Cloud-Infrastruktur, um die Geschäftskontinuität von Gesundheitseinrichtungen zu gewährleisten – einfach, flexibel und zuverlässig!

Sie wollen mehr wissen über unsere Komplettlösung für Sicherung, Wiederherstellung und Monitoring?

Kein Problem: Sprechen Sie mit den Branchen-Experten von Veeam und lassen Sie sich die Vorteile der Veeam® Availability Suite™ in all ihren Facetten präsentieren.

Rufen Sie uns an unter Tel. 0800 100 0058 oder senden Sie uns eine E-Mail an Veeam.External.Sales.EMEA.Germany@veeam.com

Sie interessieren sich für VUL, das flexible Lizenzmodell der Veeam® Availability Suite™?

Lassen Sie uns über Kosten sprechen. Ein Anruf genügt, und wir erklären Ihnen unser neues Lizenzmodell, mit dem Sie Ressourcen und Storage Kosten besser in den Griff bekommen.

Rufen Sie uns an unter Tel. 0800 100 0058 oder senden Sie uns eine E-Mail an Veeam.External.Sales.EMEA.Germany@veeam.com

Erst testen, dann entscheiden?

Das ist einfach: Unter https://www.veeam.com/de/data-center-availability-suite.html?ad=free_trial_sticky können Sie die komplette Veeam® Availability Suite™ bestehend aus Veeam Backup Replication und Veeam ONE 30 Tage lang kostenlos testen – bei vollem Funktionsumfang. Probieren Sie es aus.

Informationen zu Veeam Software

Veeam® ist ein führender Anbieter von Backup-Lösungen mit Cloud Data Management™. Mit der zentralen Plattform von Veeam können Unternehmen ihre Datensicherungsprozesse modernisieren, den Umstieg auf eine Hybrid Cloud beschleunigen und ihre Daten schützen. Mehr als 375.000 Kunden weltweit, darunter 82 % der Fortune 500- und 67 % der Forbes Global 2000-Unternehmen, und Kundenzufriedenheitswertungen auf dem 3,5-fachen Niveau des Branchendurchschnitts belegen eindrucksvoll Veeams Führungsposition auf dem Markt. Veeam ist ganz dem Channel verpflichtet und führt globale Partner sowie HPE, NetApp, Cisco und Lenovo als Exklusivhändler. Veeam betreibt Niederlassungen in über 30 Ländern.

Für weitere Informationen besuchen Sie unsere Website unter https://www.veeam.com/de oder folgen Sie uns auf Twitter unter @veeam.