Digitaler Transfer von Leistungsdaten (Teil 4): mehr Sicherheit und Effizienz heisst mehr Konzentration aufs Kerngeschäft

Innovative Partner gehören mit Sicherheit zusammen

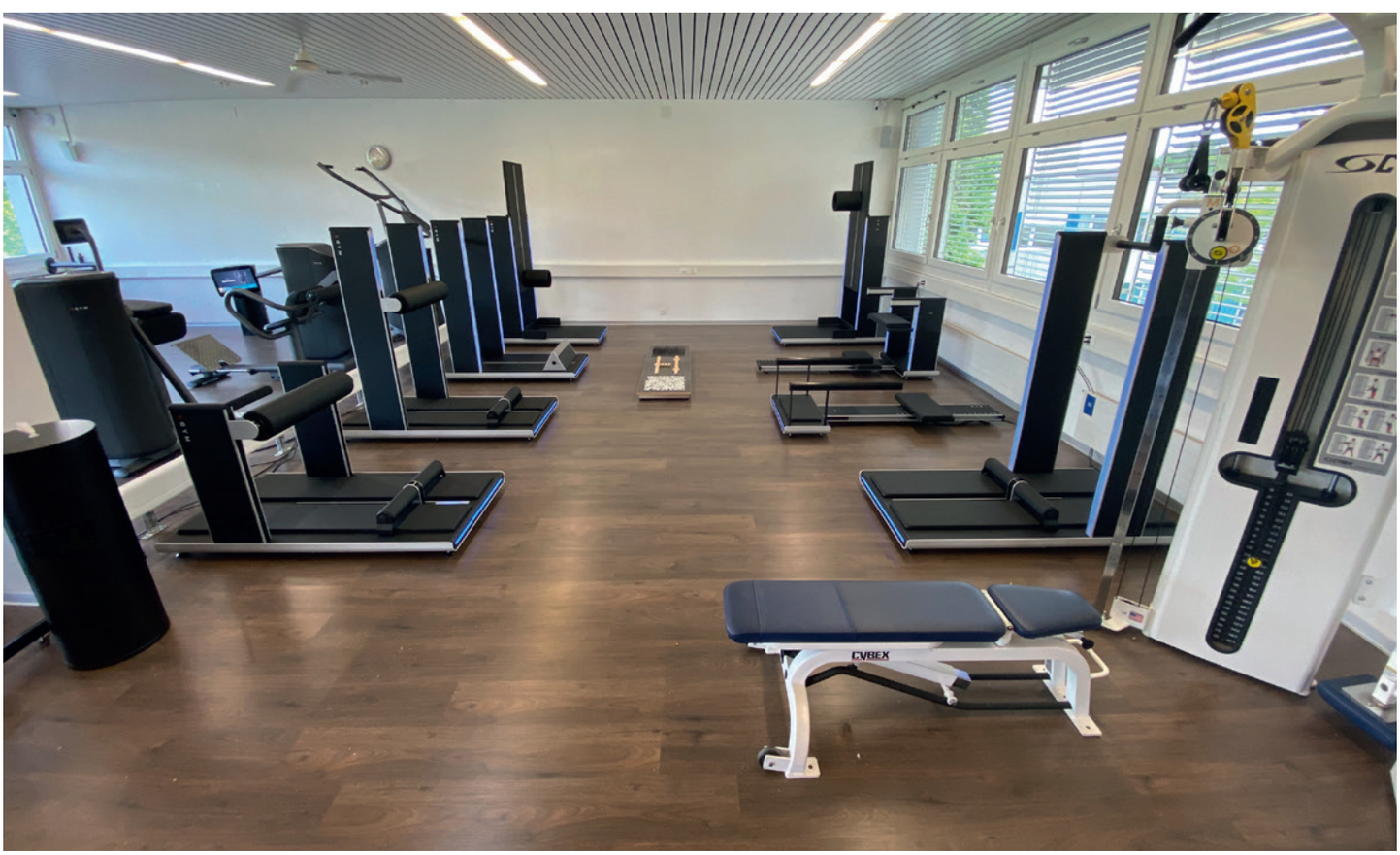
Weiterentwicklungen bewährter IT-Lösungen sind dann echt innovativ, wenn sie nebst technischen Finessen messbare Vorteile im täglichen Einsatz zeigen, wenn sie sicherer, effizienter und bedienungsfreundlicher sind. Vollblut-Unternehmer wie Ralf Senn wissen das zu schätzen.

Wenn ein leckerer Schoko-Riegel womöglich die längste Praline der Welt ist, dann könnte PlenaVita, Zentrum für Bewegung in Bülach, womöglich die modernste Physiotherapie-Praxis der Schweiz sein. Diesen Anspruch erhebt jedenfalls Geschäftsführer Ralf Senn, der während der letzten Wochen und Monate nicht nur die neusten Trainingsgeräte angeschafft hat, sondern auch seine gesamte Informationstechnik auf den neusten Stand der Technik gebracht hat. Seit sieben Wochen ist dabei das MediData-Netz im Betrieb, sehr zur Freude aller AnwenderInnen.

Gezielte Therapie und Prophylaxe

Physiotherapie, medizinische Trainingstherapie und Fitness, Rehabilitation und Prophylaxe – der Übergang ist fliessend. Beim Zentrum PlenaVita (1991-2021 Physioteam Fischer) erhalten die Patientinnen und Patienten alles professionell aus einer Hand, familiäre Atmosphäre und qualitative Betreuung inbegriffen.

Im 550 Quadratmeter grossen, modernen Therapie- und Trainingscenter fördern Qualitätsgeräte Fitness und Gesundheit. Zur Verfügung stehen sorgfältig abgestimmte und nach neuesten Erkenntnissen ausgewählte Therapie- und Trainingsgeräte. Das bedeutet ein festes Fundament, um die ideale Kombination von Rehabilitation und Prophylaxe zu schaffen. Das Training erfolgt mit wohltuendem Blick ins Grüne. Die Praxis ist an 360 Tagen im Jahr geöffnet, von 7 bis 21 Uhr – ein Erfolgsrezept, das zu einer stetig wachsenden Zahl von Patientinnen und Patienten wie auch von ZuweiserInnen geführt hat. PlenaVita beschäftigt 15 Mitarbeitende.



Problemlos und rasch ins MediData-Netz

«Weil wir innovative Therapiekonzepte pflegen, wollen wir auch im administrativen Bereich innovativ arbeiten», unterstreicht Ralf Senn. «Steht beim ersten Punkt die Gesundheit der Patientinnen und Patienten im Fokus, sind es beim zweiten Punkt Sicherheit, Effizienz und Bedienungsfreundlichkeit der IT. Wir haben sämtliche Prozesse vollständig digitalisiert und rüsten regelmässig und konsequent auf, um mit besten elektronischen Lösungen zu arbeiten. Unsere klaren Ziele sind, auch hier erstklassig arbeiten zu können, was Zeit spart – Zeit, die wiederum dank praktisch vollständiger Entlastung des Therapeutenteams von administrativer Arbeit wiederum unseren Patientinnen und Patienten direkt zugute kommt.»

Die Umstellung von MediPort zum neuen MediData-Netz erfolgte rasch und reibungslos. «Unser Software-Lieferant und die Fachleute von MediData gingen zügig ans Werk. Von Vorteil war, dass wir uns 2016 entschlossen hatten, einen Software-Wechsel vorzunehmen, um ein wesentlich leistungsstärkeres System zu nutzen. Im Einsatz steht bei uns Cenplex. An dieser kreativen Firma haben wir uns denn auch gerne beteiligt. Cenplex bietet sehr viele Funktionen, ist eine Lösung aus einem Guss und besticht durch eine ausgesprochen hohe Usability. So gab es kaum Schnittstellen zum MediData-Netz zu bearbeiten. Innert kürzester Zeit war alles via Cloud-Service implementiert und läuft seitdem zu unserer vollen Zufriedenheit.»

Schlanker Ablauf – auch dank elektronischer Kostengutsprache

Als wesentliche Vorteile nennt Ralf Senn die Schnelligkeit und umfassende Transparenz des MediData-Netzes. «Wertvoll ist auch die elektronische Kostengutsprache. Es ist ja besonders wichtig, dass beispielsweise Reha-Patienten sehr rasch ein massgeschneidertes Training beginnen können, um zur gewohnten Beweglichkeit zu gelangen resp. ihre Wiedereingliederung zu beschleunigen. Der digitale Austausch mit den Krankenversicherern erweist sich dabei als willkommener Vorteil. Dank der sehr einfachen intuitiven Bedienungsführung des MediData-Netzes können alle eKoGu wie auch sämtliche Leistungsabrechnungen höchst effizient in unserem Sekretariat abgewickelt werden. Und was ebenfalls enorm wichtig ist: Wir sind jederzeit blitzschnell über jeden einzelnen Daten- und Informationsaustausch mit Kostenträgern und weiteren Partnern im Bild, diese vollständige Transparenz schätzen wir sehr.»

Vertrauen und Integrität zum Schutz der Kunden

Exakt das war denn auch eines der grossen Anliegen von MediData beim Entwickeln des MediData-Netzes. Robert Meyer, Leiter Verkauf, hält fest: «Unsere Kunden können sämtliche Transaktionen nachverfolgen. Sie geniessen damit volle Transparenz über jeden einzelnen Datenfluss, wir hingegen haben keinen Einblick in die schützenswerten Personendaten.»

Für Robert Meyer ist zudem eines sehr wichtig: «Die sensiblen Daten sind jederzeit vollständig geschützt. Damit erfüllen wir eine wichtige Sorgfaltspflicht gegenüber unseren Kunden und erfüllen so auch die strengen Datenschutzauflagen des Bundes. Auf diese Weise können sie sich auf einen einfachen, sicheren und unveränderten Datenaustausch verlassen. Ein anderweitiges Verwenden von Daten ist organisatorisch und technisch ausgeschlossen. Das Einhalten dieser Sicherheits- und Qualitätskriterien wird jährlich in Aufrechterhaltungs-Audits und alle drei Jahre in einer umfassenden ISO 27001 Re-Zertifizierung überprüft. Dabei werden bei MediData nicht bloss einzelne Prozesse zertifiziert, sondern jeweils die gesamte Firma.»

Sichere, eigenständige Weiterentwicklung

Und wie finden angesichts des erfreulichen Wachstums von MediData (wir berichten in dieser «clinicum»-Ausgabe über das erfreuliche Geschäftsjahr 2020 und die GV des Unternehmens) IT-Weiterentwicklungen statt? – «Mit dieser Aufgabe sind drei Teams betraut, die alles Firmenspezifische entwickeln», erläutert Robert Meyer. «Wir nehmen auch hier den Datenschutz bei jedem Schritt sehr ernst. Beispielsweise leisten wir uns den Aufwand, Testdaten vollständig synthetisch herzustellen und gewinnen sie nicht einfach aus produktiven Daten. Im eigentlichen IT-Betrieb ist die Entsorgung ein besonders heikles Thema. Obwohl die Daten auf den Datenträgern verschlüsselt sind, werden defekte oder ausrangierte Datenträger fachmännisch mit einem HDShredder vernichtet und entsorgt. Kompromisse sind hier ausgeschlossen.»

Cybersecurity hat höchste Priorität

Gerade hier gilt auch: Das Bessere ist der Feind des Guten. «IT-Sicherheit wird immer komplexer», betont Robert Meyer, «insbesondere im Gesundheitswesen. Daher arbeiten wir ständig daran. Unsere Antwort ist insbesondere die Strategie der Dynamischen Verteidigung. Ausgangsbasis unserer laufenden Analysen ist die zunehmende Vernetzung des Geräteparks von Gesundheitseinrichtungen; Fehlfunktionen von Geräten bedrohen die Gesundheit oder gar das Leben der Patienten. Weiter besteht eine heterogene IT-Infrastruktur in den Spitälern, Labors und Praxen – und leider gibt es kaum verbindliche

Ralf Senn, Geschäftsführer Zentrum PlenaVita GmbH, Bülach

Robert Meyer, Leiter Verkauf, MediData AG

Normen und Mindeststandards bezüglich IT-Sicherheit. Andererseits führt die Sensibilisierung der Öffentlichkeit auf das Thema Datenschutzverletzungen immer schneller zu Imageschäden.

Je lebenswichtiger IT-Sicherheit für eine Organisation ist, desto anfälliger ist diese zudem auch für Erpressungsversuche durch Cyberkriminelle. Die höchste bislang bekannt gewordene Lösegeldforderung in der Schweiz beträgt immerhin 6 Mio. Franken! Tendenz steigend.»

Advanced Persistent Threats

Cyberattacken sind längst nicht mehr das Tummelfeld von «Nerds», sondern das Geschäft bestens ausgebildeter, straff organisierter krimineller Organisationen. Sicherheitsexperten sprechen in diesem Zusammenhang von «Advanced Persistent Threats» (APT). Gemeint sind professionelle Angriffe auf der Basis massiver Ressourcen, von langer Hand vorbereitet und mit einem klaren Business-Ziel: Erpressen von Lösegeld, Spionage usw.

Eine Konsequenz dieser Professionalisierung von Cyberattacken ist mit gezielten Vorkehrungen die Systeme entsprechend zu schützen. Dabei ist ein Bündell an Massnahmen intelligent und mehrstufig auf zu bauen und zu verknüpfen. Besonderer Bedeutung kommt hier vor allem der aktiven Überwachung der Systeme auf mögliche Cyberattacken zu.

Strategie der Dynamischen Verteidigung

Die klassischen Sicherheitskonzepte können moderne Cyberattacken im Stile von APT nicht mehr genügend abwehren. Es reicht heutzutage nicht mehr, Firewall und Virenscanner zu installieren und regelmässig zu aktualisieren. Dazu ist die IT-Landschaft zu komplex und ändert sich zu schnell. Die moderne Cybersecurity arbeitet darum nach der Strategie der Dynamischen Verteidigung. Deren Prinzipien lauten:

- **Ständige Aktualisierung:** Monitoring neuer Bedrohungen und laufendes Update der Abwehrsysteme (Firewall, Gateways, Betriebssysteme usw.)
- **Isolation:** Trennung der Produkte/Systeme durch zwischengeschaltete Kontroll-Instanzen, um eine gegenseitige «Kontaminierung» zu vermeiden. Besonders wichtig ist hierbei die Isolation älterer Systeme, die nicht regelmässig aktualisiert werden (Beispiel: PCs, die noch unter Windows 7 laufen)
- **Authentisierung und Autorisierung:** Im Rahmen einer Authentisierung erbringt eine Person oder System den Beweis dafür, dass sie ist, wer sie zu sein vorgibt.Bei der Autorisierung erfolgt das Gewähren des Zugangs zu den Privilegien, welche der erfolgreich nachgewiesenen Identität zustehen.
- **Verschlüsselung:** Alle Datenströme werden verschlüsselt, sodass Sicherheitslecks im Netzwerk nicht zur Preisgabe von Informationen führen. Hierzu werden spezielle zertifikatsbasierte Systeme genutzt. Ein Zertifikat enthält einen öffentlichen Schlüssel und bindet diesen an die Identität einer Person, eines Computers oder eines Diensts mit dem entsprechenden privaten Schlüssel. Öffentliche und private Schlüssel werden vom Client und vom Server zum Verschlüsseln von Daten vor deren Übertragung verwendet.

Das Sicherheitskonzept des MediData-Netzes

Das MediData-Netz setzt die Strategie der Dynamischen Verteidigung konsequent um. Der Einsatz von Nevis für die Authentisierung und Autorisie-

Bei PlenaVita freut man sich über das bedienungsfreundliche MediData-Netz – so bleibt mehr Zeit für die Betreuung der Patienten.

rung (Identity und Access Management (IAM)) sowie ein zertifikatsbasiertes Daten-Verschlüsselungsverfahren bilden den Kern des Sicherheitskonzeptes. Das Softwareprodukt Nevis der Firma Adnovum sorgt für maximalen Schutz vor fremdem Eindringen in das MediData-Netz. Adnovum zählt zu den führenden Spezialisten für Cybersecurity – auch Banken, die Post oder der schweizerische Zoll vertrauen auf die Lösung von Adnovum. Die Firma analysiert laufend Internetbedrohungen und aktualisiert die Software entsprechend. Zudem werden die Systeme über Firewalls und Netzwerksegmentierung isoliert sowie durch weitere Massnahmen wie Penetrations-Tests, System-Monitoring, Redundanz, Virenscanner etc. laufend überwacht und geschützt. Die MediData Appliance – ein autonomer Mini-PC oder als «Virtual-Machine» (VM) – wird zwischen das eigentliche Netzwerk und den PC der Arztpraxis geschaltet (Prinzip der Isolation). Die Appliance wird von MediData direkt über das Internet mit den Updates (Prinzip der periodischen Aktualisierung) regelmässig aktualisiert und so mit den neusten Sicherheits-Updates bestückt.

Die Appliance kommuniziert mit der Branchensoftware über ein REST API mit Authentisierungsschlüssel, um Daten ins Netz hochzuladen bzw. Informationen abzufragen. Eine Praxis kann so zum Beispiel 5 PCs betreiben, die untereinander vernetzt sind und alle sicher auf die MediData Appliance zugreifen. Die gesamte Kommunikation zwischen dem PC der Arztpraxis und der Box sowie zwischen der Box und dem Internet ist verschlüsselt (TLS).

Maximale Ausfallsicherheit

Netzwerkausfälle werden durch die MediData Appliance sicher abgefangen. Ein Datenverlust ist somit praktisch ausgeschlossen.

Hinzu kommt, dass das MediData-Netz doppelt geführt wird: Es gibt nicht nur ein, sondern zwei parallele Datencenter, die untereinander mit Glasfaser-Kabeln verbunden sind. Sollte ein Datencenter einmal ausfallen, würde das andere dessen Betrieb nahtlos weiterführen, ohne dass die AnwenderInnen davon etwas bemerken.

Robert Meyer: «Security kann man nicht kaufen – man muss ständig dafür Sorge tragen. Es gibt kein Produkt ab der Stange, das automatisch ein Netzwerk absichert. Vielmehr muss Sicherheit durch genaue Analyse und geschickte Kombination verschiedener Elemente hergestellt werden. Im Falle des MediData-Netzes durch die Kombination externer Cybersecurity (Nevis/Adnovum), Hochsicherheits-Datencenter und die MediData Appliance mit entsprechenden Software-Schnittstellen. Doch auch die klügste Kombination nützt nichts, wenn sie als statische ‹Sicherheitsmauer› gedacht ist. Nur ein dynamisches System, das sich laufend auf neue Konstellationen und Bedrohungen einstellt, kann den professionellen Cyberattacken der heutigen Zeit die Stirne bieten.»

Für User wie Ralf Senn und sein Team von PlenaVita geben die ständigen Efforts für höchste Sicherheit ein gutes Gefühl: «Wir wissen, dass wir uns auf innovative Lösungen von MediData verlassen können. Es ist schon so: Innovative Partner gehören mit Sicherheit zusammen.»

Weitere Informationen

www.medidata.ch
www.plenavita.ch

PlenaVita bietet eine ganzheitliche Betreuung und Therapie für ihre Patienten. Die innovative Arbeitsweise des Unternehmens und das innovative MediData-Netz passen prima zusammen.