Entscheidende Elemente für mehr Datensicherheit im Gesundheitswesen

MediData: sicher und nachhaltig – ein gutes Gefühl

Kaum woanders existieren dermassen viele sensible Daten, die höchsten Persönlichkeitsschutz verlangen, wie im Gesundheitswesen. Zudem ist hier das Moorsche Gesetz, nach dem sich die Datenmenge alle 18 Monate verdoppelt, hautnah zu spüren. Innovative bildgebende Verfahren, die wachsende Vernetzung der einzelnen Akteure und generell die zunehmende Digitalisierung schaffen enorme Datenmengen, die vermehrt sicher ausgetauscht werden müssen. Kompromisslose Sicherheit ist unverzichtbar. Welche Herausforderungen sich dabei ergeben, wollten wir bei MediData erfahren, deren Fachleute im Dienste des Datentransfers stehen.

«Sicherheit bei MediData ist grundsätzlich immer eine doppelte», betont Daniel Bätschmann, Stellvertretender CEO und Informatikleiter. «Einerseits unterhalten wir an unserem Firmensitz in Root eine Informationstechnik, die stets auf dem neusten Stand ist und für die höchste Sicherheitsstandards gelten. Dabei geht es insbesondere um den Datenzugriff, eine unterbrechungsfreie Stromversorgung und Klimatisierung. Andererseits unterhalten wir seit August 2015 in einem Datacenter der CKW Fiber (einer Tochtergesellschaft der Centralschweizerischen Kraftwerke CKW) eine Co-Location, in der sämtliche in Root vorhandenen Daten unter gleichermassen strengen Auflagen gespiegelt werden. Die Dienste dieser leistungsstarken Einrichtung nehmen auch der Kanton Luzern und das Luzerner Kantonsspital in Anspruch. Die Verbindung wird mit Darkfiber-Glasfasern sichergestellt. Wir sehen diese doppelte Sicherheit als entscheidendes Element unseres Business Continuity Managements im Rahmen der ISO-27001 / VDSZ-Zertifizierungen. Wir überlegen uns dabei immer wieder: Welche Szenarien könnten eintreten? Wie lange wäre es im Extremfall denkbar, dass kein Datenzugriff möglich wäre?»

Daniel Bätschmann, Stellvertretender CEO und Informatikleiter

Höchste Sicherheit von Anfang an

Bevor mit der Co-Location ein Daten-Storage an einem weiteren Standort eingerichtet wurde, bestand bereits ein zweiter Serverraum in Root. «Beide Räume», so Daniel Bätschmann, «waren natürlich von Anfang an erstklassig gegen Stromausfall, Feuer oder Wasser geschützt. Aufgrund unseres Wachstums wollten wir allerdings einen wichtigen Schritt weiter gehen. Selbst wenn nun beide bisherigen Serverräume vorübergehend ausfallen sollten, wäre mit der Co-Location dafür gesorgt, dass wir in kürzester Zeit wieder online sind. Darauf können sich unsere Kunden verlassen. Für die Zukunft sind wir gerüstet.»

Die Sicherheit beginnt bei den Mitarbeitenden

Modernste Informationstechnik ist das eine, das Verhalten der Mitarbeitenden das andere. «Ich betrachte es als das entscheidende Fundament, denn der während der letzten Jahre stark gestiegene Transfer sensibler Daten aus dem Gesundheitswesen verlangt eine lückenlose Sicherheit auf allen Ebenen. Deshalb lautet unser Sicherheits-Credo: Wir wollen das uneingeschränkte Vertrauen unserer Kunden gewinnen, der Leistungserbringer in Spital, Praxis, Apotheke oder Labor, und selbstverständlich auch der Patienten, die sie betreuen. Alle sollen jederzeit gewiss sein, dass mit ihren Daten nie

etwas passiert. Falsche, nicht autorisierte Zugriffe dürfen nicht vorkommen. Deshalb stellen wir mit einen PKI-Verfahren sicher, dass Sender und Empfänger von Daten in jedem Fall tatsächlich die richtigen sind.

Unsere Mitarbeitenden wissen, dass es entscheidend ist, dass unserer Tätigkeit ohne jede Einschränkung vertraut werden kann. Die Integrität unserer Fachleute ist gleich wichtig wie die technische Sicherheit. Wir verstehen uns denn auch in unserer täglichen Aufgabe als Treuhänder unserer Kunden.»

Laufende Schulung, Information und Weiterbildung

Alle Mitarbeitenden werden bei ihrem Firmeneintritt wie auch während ihrer Anstellung regelmässig bezüglich Informationssicherheit und Datenschutz geschult. «Sicherheit ist bei uns ein Dauerthema mit vielen Facetten. Wir wollen, dass unsere Kunden bei jedem Kontakt mit unseren Mitarbeitenden spüren, dass bei uns ein uneingeschränktes Klima der Sicherheit herrscht», unterstreicht Bätschmann. «Diese Firmenphilosophie gilt für alle, obwohl es nur ganz wenige Mitarbeitende sind, die direkten Zugang zu unseren IT-Systemen haben. Wir setzen viel daran, dass unsere Mitarbeitenden motiviert sind, in sicherheitsrelevanten Aspekten mitzudenken. Das bedeutet, diese Aspekte zu verstehen, Verständnis dafür zu haben und zu wissen, dass es allen nützt. Sämtliche relevanten Themen werden stufengerecht und funktionsbezogen vermittelt. Erfolgen Änderungen in der Sicherheitslandschaft und den entsprechenden Dokumenten, werden sie sofort mitgeteilt, ebenso aktuelle Bedrohungen wie sie Hacker-Angriffe bedeuten können. Ein monatlicher interner Newsletter schliesst den Reigen stetiger Informationen ab. All diese Massnahmen zu Gunsten unserer Mitarbeitenden erachten wir als eine besonders wichtige Investition.»

Vertrauen und Integrität zum Schutz der Kunden

MediData-Kunden können sämtliche Transaktionen nachverfolgen. Kunden geniessen damit volle Transparenz über jeden Datenfluss, «wir hingegen», so Daniel Bätschmann, «haben keinen Einblick in die schützenswerten Personendaten.»

Wichtig ist ein weiterer Service. Etliche Arztpraxen rechnen über MediData nach dem Tiers garant-System ab. Hier müssen die Leistungsabrechnungen, grossmehrheitlich per Post, rasch zu den Patienten versandt werden. Ein

Anita de Jong, Software-Entwicklerin und Sicherheits-Beauftragte

Rollen-Druckservice führt direkt zu einer automatisierten Verpackungsanlage und von dort sofort in den Versand.

Für den Informatik-Chef ist klar: «Wir wollen jederzeit selber wissen, wo die Daten sind. Damit erfüllen wir eine wichtige Sorgfaltspflicht gegenüber unseren Kunden. Diese können sich auf einen einfachen, sicheren und unveränderten Datenaustausch verlassen. Gerade transparente überschaubare Abläufe erleichtern die Zusammenarbeit und schaffen auf diese Weise einen weiteren Aspekt von Sicherheit. Kundendaten müssen stets, zu jeder Tages- und Nachtzeit, für sie verfügbar sein. Ein andersweitiges Verwenden von Daten muss organisatorisch und technisch ausgeschlossen werden. Das Einhalten dieser Sicherheits- und Qualitätskriterien wird jährlich in Aufrechterhaltungs-Audits und alle drei Jahre in einer umfassenden Re-Zertifizierung überprüft. Zu beachten ist: Bei uns werden nicht bloss einzelne Prozesse zertifiziert, sondern die gesamte Firma.»

Sichere, eigenständige Weiterentwicklung

Und wie finden angesichts des erfreulichen Wachstums von MediData IT-Weiterentwicklungen statt? – Mit dieser Aufgabe sind drei Teams betraut, die alles Firmenspezifische entwickeln. «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, wird einer qualifizierten Vernichtung defekter oder ausrangierter Teile grösste Beachtung geschenkt. Kompromisse sind hier ausgeschlossen», betont Bätschmann.

Schliesslich ist das Stichwort Internet-Security nicht zu vergessen. «Oft ein komplexes Gebiet für unsere Kunden», räumt unser Interviewpartner ein, «hier unternehmen wir alles, um bei unsern über 8000 Vertragspartnern hart dran zu bleiben und gerade kleine Leistungserbringer wirksam zu unterstützen, damit bei ihnen weder Risiken noch Informationslecks entstehen.»

Gut organisiert – gut geschützt

Anita de Jong, Software-Entwicklerin und Sicherheits-Beauftragte, teilt die Meinung des Infor-

Auf Nummer sicher: Alle Daten, die hier in Root entstehen, werden mit grösster Sorgfalt auch in der Co-Location gespiegelt.

matikchefs: «Sicherheit beginnt bei jeder und jedem Einzelnen. Und dafür braucht es eine entsprechende Organisation.» – Ein solides Fundament bildet das Gremium für interne Sicherheit (GIS), das aus der dreiköpfigen Geschäftsleitung und unserer Gesprächspartnerin besteht. Das GIS ist für die Sicherheits-Strategie verantwortlich. Hier werden Richtlinien festgelegt und top down im Unternehmen gelebt. Im Sicherheits-Alltag übernimmt das Kern-Team Daniel Bätschmann und Anita de Jong die Führung, das alle Aufgaben sorgfältig auslotet, plant und priorisiert. «Rechtzeitig das Richtige tun, lautet die Devise. Hier geht es neben dem Datentransfer mit den Kunden auch ums firmeneigene digitale Managementsystem und das Dokumentieren entsprechender Daten, beispielsweise aus dem Finanz- und Rechnungswesen.»

Das GIS tritt regelmässig zusammen. Sorgfältig wird überprüft, wie der Stand aller IT- und Sicherheitsprojekte ist, ob die Teams mit ihrer Arbeit gut vorankommen, ob aufgrund technischer Entwicklungen oder des Firmenwachstums neue Priorisierungen nötig werden, ob Leistungen ausgebaut werden müssen, um eine hohe Performance zu garantieren, und nicht zuletzt, was von aussen auf MediData zukommt. Impulse können hier durch neue Regulatorien, Kundenanforderungen oder eHealth-Lösungen ausgelöst werden.

Nachhaltig mit klaren Sicherheitszielen

Bei der regelmässigen grundlegenden Auslegeordnung geht es um die vielen Facetten der Informationssicherheit wie Vertraulichkeit, Integrität sowie hohe Verfügbarkeit von Informationen, Daten und Systemen. Ebenso wichtig ist dabei der eigentliche Datenschutz unter Einhaltung aller gesetzlichen Auflagen. «Wir wollen die Effektivität der IT-Sicherheit durch konsequentes Planen, Umsetzen, Kontrollieren und, wo nötig, Korrigieren laufend verbessern. Dafür setzen wir interne wie externe Audits ebenso ein wie regelmässige Risikoanalysen, Massnahmenüberprüfungen, Kontrollen von Aufzeichnungen und Auswertungen von Sicherheitsvorfällen.»

Für den Bereich des Datenschutzes gelten gleichermassen harte Vorgaben. Es müssen sämtliche dafür nötigen Prozesse und Massnahmen fürs Einrichten, Umsetzen, Durchführen, Überwachen, Überprüfen, Instandstellen und kontinuierliches Verbessern optimal aufgebaut und betrieben werden.

«Kompromisslose Sicherheit, wie sie insbesondere mit dem Aufbau der Co-Location zum Ausdruck gelangt, und permanente Kontrollen behalten oberste Priorität. Gleichzeitig sorgen wir auch eindeutige Stellvertretungen unter den Mitarbeitenden, das Wissen soll im Unternehmen bleiben, Weiterbildung stärkt es. Und schafft die beste Voraussetzung für Konstanz und Nachhaltigkeit, denn», darauf zählen Daniel Bätschmann wie Anita de Jong, «Sicherheit ist ein Dauerthema und wird es bei uns auch immer bleiben.»

Text: Dr. Hans Balmer

MediData – für eine gesunde Entwicklung im Schweizer Gesundheitswesen

MediData ist ein massgebender Informatik-Dienstleister für elektronische Gesundheitsdienste in der Schweiz und in angrenzenden Regionen. Die 62 Fachleute des Unternehmens bringen mit effizienten IT-Lösungen Leistungserbringer (Ärzte, Apotheken, Spitäler, Labors, Pflegheime, Spitex etc.), Kranken- und Unfallversicherer, Kantone sowie Patienten zusammen. Das klare Ziel ist die Vernetzung aller Beteiligten im Schweizer Gesundheitswesen und somit das Ermöglichen eines effizienten Informationsaustausches und Sicherstellen optimaler Prozesse.

Kunden und Partner schätzen an MediData:
- **Sicherheit** (zertifiziert nach ISO 27001 und VDSZ)
- **Erfahrung** (über 20 Jahre etabliert im Schweizer Gesundheitswesen)
- **Qualität** (nachhaltige Werte: Respekt, Loyalität, Klarheit, Verlässlichkeit und unternehmerisches Handeln)
- **Support** (persönliche Betreuung – der Mensch steht im Mittelpunkt)
- **Know-how** (ausgeprägte Kompetenz und Erfahrung durch Spezialisten, die bereits 10 und mehr Jahre bei MediData tätig sind)