MediData zeigte an der GV ausgeprägten Innovationsgeist und die Bereitschaft, komplexe Aufgaben zu meistern

Verlässlicher Partner im rasanten Wandel des Gesundheitssystems

Das Schweizer Gesundheitssystem befindet sich in einem ausgeprägten Strukturwandel – technologisch, regulatorisch und gesellschaftlich. Inmitten dieser Dynamik steht ein Unternehmen für Kontinuität: Mit einem gesunden Geschäftsjahr 2024 unterstreicht MediData seine Rolle als verlässlicher Partner für eine sichere, digitale und zukunftsfähige Gesundheitsversorgung.

«MediData hat sich als feste Grösse im Schweizer Gesundheitssystem etabliert. Diese Entwicklung weiterzuführen und zu stärken, ist eine grosse Verantwortung», sagte Dr.iur. German Grüniger, Präsident des Verwaltungsrates, an der Generalversammlung. MediData gestaltet die digitale Transformation mit – durch einen sicheren und zukunftsgerichteten Datenraum, der den Austausch zwischen über 22 000 angeschlossenen Akteuren im Gesundheitssystem ermöglicht. «Wir setzen auf Innovation und höchste Sicherheitsstandards, um Prozesse zu vereinfachen, die Zusammenarbeit zu fördern und einen Beitrag zur Stabilität des Systems zu leisten», so Grüniger.

Ein Datenraum, der verbindet

Das Unternehmen aus Root mit seinen 95 Mitarbeitenden trägt wesentlich dazu bei, das Gesundheitssystem effizient, sicher und vernetzt zu gestalten. 100 % der Krankenversicherer (KVG/VVG), 99 % der Unfallversicherer, 98 % der Apotheken, 95 % der Spitäler, 81 % der Labore sowie alle 26 Kantone sind heute Teil des MediData-Netzes. Auch rund 8700 Ärztinnen und Ärzte, über 760 Spitex-Organisationen und mehr als 1100 Alters- und Pflegeheime nutzen den Datenraum. Im Jahr 2024 wurden insgesamt 105.8 Millionen elektronische Dokumente übermittelt. Der Umsatz betrug CHF 39.263 Millionen.

Kontinuität in der Führung

An der Generalversammlung hiessen die Aktionärinnen und Aktionäre sämtliche Anträge des Verwaltungsrats gut: Sie genehmigten den Lagebericht und die Jahresrechnung 2024, stimmten der Gewinn- und Reservenverwendung zu und entlasteten die Mitglieder des Verwaltungsrats sowie der Geschäftsleitung. Die KPMG AG, Luzern, wurde für das Geschäftsjahr 2025 einstimmig als Revisionsstelle bestätigt. Anne-Geneviève Bütikofer, Andreas Dummermuth und Benno Fuchs wurden für eine weitere Amtsdauer von drei Jahren als Mitglieder des Verwaltungsrats wiedergewählt.

Cybersecurity ist wichtiger denn je. Kriminelle greifen immer gezielter auf wertvolle Daten zu und entwickeln dabei eine unheimliche Dynamik und Raffinesse. Vorbeugen ist unverzichtbar.

Ernesto Hartmann von InfoGuard liess mit seinem Gastreferat aufhorchen: Dunkle Kräfte sind emsig am Daten stehlen, und das leider mit Erfolg.

Sicherheit schafft Vertrauen

«Das Transportvolumen ist 2024 erstmals in den dreistelligen Millionenbereich gestiegen – und wir haben die Marke von 20'000 Anschlüssen überschritten», unterstrich CEO Daniel Ebner. «Doch für uns geht es nicht um Zahlen allein. Sicherheit ist die Grundlage für Vertrauen – und Vertrauen ist die Basis für eine digitale Gesundheitsversorgung, die funktioniert. Mit der ISO 27001-Zertifizierung und der Datenschutz-Zertifizierung nach VDSZ setzen wir Standards im Umgang mit Gesundheitsdaten. Unsere Lösungen entwickeln wir kontinuierlich weiter – nicht um ihrer selbst willen, sondern weil ein verlässlich vernetztes Gesundheitssystem allen Beteiligten zugutekommt und letztlich die Lebensqualität in der Schweiz stärkt.»

Daten sind kostbar und verlockend

Nicht nur der Strukturwandel im Gesundheitswesen schreitet rasant voran, auch die Datenmengen, die täglich genutzt und sicher archiviert werden müssten, nehmen im Eilzugstempo zu. Gleichzeitig wachsen Gesundheitsdienstleister zusammen und vernetzen sich. Administrative wie medizinische Prozesse werden komplexer und mit der Künstlichen Intelligenz und der personalisierten Medizin wachsen gewaltige Quellen neuer Daten heran. Kein Wunder wecken diese wertvollen Daten auch das Interesse dunkler Gestalten. Wie bedrohlich dieses Szenario ist, präsentierte Gastreferent Ernesto Hartmann, Chief Cyber Defence Officer der marktführenden Schweizer Cybersecurity-Firma InfoGuard.

Cyberkriminalität ist ein eigentliches Geschäftsmodell geworden, und es floriert ungeniert. Mit einem Umsatzvolumen weltweit von 9.5 Billionen Dollar ist das dunkle Geschäft zur drittgrössten «Volkswirtschaft» geworden; nur China mit 17.9 Billionen und die USA mit 27.9 Billionen Dollar sind noch mächtiger. Die Hackerangriffe machen erwartungsgemäss auch vor Schweizer Unternehmen und Institutionen nicht Halt. Das zeigen eindrückliche Zahlen aus dem InfoGuard Computer Security Incident Response Team (CSIRT). «Hohe Fallzahlen aus dem Security Operations Center (SOC) und dem CSIRT ermöglichen uns tagesaktuelle Informationen über die Bedrohungslage», so Ernesto Hartmann. «2023 waren es schweizweit 260 Vorfälle, 2024 deren 264 und während der ersten vier Monate 2025 waren es bereits 137, Tendenz steigend. Jeder Cyberangriff ist eine Warnung, wir müssen handeln und lernen.»

Immer raffinierte Angreifer bedrohen immer mehr auch kleinere Betriebe

Dieser Ratschlag ist sehr wichtig, denn die Angreifer werden immer raffinierter und organisieren sich gezielt. Sie beschaffen sich nicht nur Daten, die für einen Angriff lohnend erscheinen, via Darknet, sondern unterhalten auch Initial Access Broker-Systeme und umfangreich dotierte Entwicklungszentren. Die Hacker sind leider sehr erfolgreich und nehmen auch zunehmend kleinere Betriebe, die erfahrungsgemäss einen weniger ausgebauten IT-Schutz implementiert haben, ins Visier. Das traf insbesondere 2024 zu. Die betroffenen, oft kleineren Unternehmen, die aufgrund zerstörter Backups häufig gezwungen waren, Lösegeld zu zahlen, überwiesen letztes Jahr 2.2 Mio. Dollar an Kriminelle. Das entsprach 28 % aller geforderten Summen, 2023 waren es erst 18 %. Leider geht der Trend geht weiter. Von Januar bis Ende April 2025 wurden 26 Ransomware Incidents durch das InfoGuard CSIRT bearbeitet. Dabei wurde bereits eine Lösegeldsumme von 3.8 Mio. Dollar überwiesen. Die grössten Angriffsflächen für einen kriminellen Einstieg in die Datenbasen lieferten Intentionen, die auf Identitäten abzielten.

Nach wie vor stellen Phishing-E-Mails eine grosse Gefahrenquelle dar. Ernsto Hartmann berichtete von einem sehr ernsten Fall, bei dem ein Phishhing-E-Mail einen Hyperlink zu einer kompromittierten Website enthielt, der dazu diente, Microsoft 365-Zugangsdaten auszuspähen und Session-Cookies zu stehlen. Mittels Authentifizierungs-Bypass und MFA-Umgehung wurde es möglich, das gestohlene Session-Cookie, den Authentifizierungsprozess zu umgehen, selbst wenn bei den Nutzern die Multi-Faktor-Authentifizierung (MFA) aktiviert ist. Sicherheitsmassnahmen wie MFA werden dadurch ausgehebelt und unautorisierter Zugriff wird möglich.

Enormen Schäden vorbeugen

Ein kleiner Lichtblick kann unter Umständen darin bestehen, dass sich die professionellen Datendiebe gewisse «ethische» Richtlinien gegeben haben. Diese enthalten etwa einen Verzicht auf Angriffe auf Daten in bestimmten, meist öst-

Im Gesundheitswesen nimmt die Datenflut rasant zu, ebenso die Vernetzung und die Komplexität von Prozessen. All das erfordert eine lückenlose sicherheitstechnische Prophylaxe.

Daniel Ebner, CEO, und Dr. German Grüniger, VR-Präsident von MediData, freuen sich am erreichten Wachstum, der soliden Finanzierung und der erfolgreich verlaufenden innovativen Projekte.

lichen Ländern, oder eine Rücksichtnahme auf Non Profit-Organisationen oder Spital-Infrastrukturen, die lebenserhaltend und unverzichtbar sind. Verlass darauf ist allerdings nicht in jedem Fall gegeben. Vorzubeugen lohnt sich unvermindert, denn auch ein kurzfristiger Unterbruch in einem Klinikbetrieb kann verheerend sein, enorme Kosten auslösen und einen bedeutenden Reputationsverlust bewirken. Ernesto Hartmann berichtete von Häusern, die tagelang auf Papier umsteigen mussten und nach Behebung der Hacker-Krise ihre Systeme wieder mit einem gewaltigen Aufwand hochfahren mussten.

Abschliessend meinte daher der Experte: «Im IT-Bereich haben wir privilegierten Zugriff auf kritische Systeme und Daten. Es ist unsere Pflicht, diese Ressourcen sicher und verantwortungsvoll zu verwalten.» Das tun die 90 InfoGuard-Spezialsten für über 400 Kunden.

Sicherheit gehört zur DNA von MediData

Der Cybersecurity widmet auch MediData – unterstützt von InfoGuard – seit Langem grösste Aufmerksamkeit. Eine der wichtigsten Massnahmen ist, dass bei Kunden nur autorisierte Personen auf sensible Daten zugreifen können. Innerhalb des MediData-Netzwerks sind die einzelnen Anwendungen – darunter das Kundenportal, in dem Kunden ihre Einstellungen konfigurieren können, und das interne Tool der Supportabteilung – vollständig geschützt. BenutzerInnen authentifizieren sich mittels eines Zertifikates, das ein Schlüsselpaar enthält, während der Zugriff über ein automatisch erneuertes Zugangstoken erfolgt. Mit der gewählten Lösung lassen sich den BenutzerInnen, die mehrere Einheiten abdecken, unterschiedliche Rollen zuweisen.

Auch die MediData-IT-Infrastruktur und -Organisation unterliegt höchsten Sicherheitsanforderungen. Sie wird nonstop à jour gehalten und zertifiziert, erst kürzlich fanden erfolgreiche Audits für ISO 27001:2022 und VDSZ:2023 statt. IT-Sicherheit bleibt ein wichtiges Thema für die Zukunft. Darüber hinaus, wie CIO Bernhard Joos an der GV erläuterte, wird das Unternehmen, das mittlerweile 95 Mitarbeitende beschäftigt, auch in den kommenden Jahren die Digitalisierung des Schweizer Gesundheitssystems vorantreiben: «Um neuste Entwicklungen und Anforderungen des Marktes frühzeitig zu erkennen, haben wir das Instrument des Trendradars kreiert. Ein wichtiger Schwerpunkt für die Zukunft liegt in der Weiterentwicklung des MediData-Netzes. 2024 haben viele Softwarehäuser und deren KundInnen auf den neuen Webservice umgestellt. 2025 wird diese Umstellung abgeschlossen sein, wodurch der Zugang für alle Leistungserbringer zum MediData-Netz direkt aus der Klinik- oder Praxissoftware möglich wird – dank eines Zertifikats und ohne zusätzliche physische Hardware.

Darüber hinaus investieren wir in die Weiterentwicklung unserer Tariflösungen, um unseren Partnern langfristig eine solide Basis für die Leistungsprüfung zu gewährleisten. Wir unterstützen die Umstellung des XML-Rechnungsstandards 5.0 des Forums Datenaustausch, um die elektronische Kommunikation und Abrechnung im Gesundheitssystem noch effizienter und transparenter zu gestalten. Dies betrifft die neuen ambulanten Arzttarife (TARCOD und ambulante Pauschalen) sowie erweiterte Inhalte, was allen Akteuren des Gesundheitssystems zugutekommt.

Erfolgreich eingeführt wurde seit April 2022 das Patientenportal, das rege genutzt wird. Bis heute wurden bereits über 26 Millionen Abrechnungsdokumente sicher übermittelt. Das Patientenportal verzeichnet weiterhin ein starkes Wachstum: Die Anzahl der Transaktionen ist im Vergleich zum Vorjahreszeitraum um nahezu 27 % gestiegen. Schliesslich engagieren wir uns im Bereich der Interoperabilität und laden alle Partner im Gesundheitssystem ein, gemeinsam Lösungen zu entwickeln, die das gesamte Ökosystem stärken.»

Weitere Informationen

www.medidata.ch