Lors de l'assemblée générale, MediData a fait preuve d'un fort esprit d'innovation et d'une volonté de maîtriser des tâches complexes

Un partenaire fiable pour la transformation rapide du système de santé

Notre système de santé connaît une profonde mutation structurelle, tant sur le plan technologique que réglementaire et sociétal. Face à cette dynamique, une entreprise incarne la continuité: avec un exercice 2024 prospère, MediData confirme son rôle de partenaire fiable pour toutes les données sécurisées, numériques et pérennes du systéme de santé.

«MediData s'est imposé comme un acteur clé du système de santé suisse. Poursuivre et consolider ce développement est une grande responsabilité », a déclaré le Dr iur. German Grüniger, président du conseil d'administration, lors de l'assemblée générale. MediData contribue à façonner la transformation numérique grâce à un espace de données sécurisé et tourné vers l'avenir, permettant l'échange entre plus de 22'000 acteurs connectés au réseau MediData. «Nous misons sur l'innovation et les normes de sécurité les plus strictes pour simplifier les processus, favoriser la collaboration et contribuer à la stabilité du système», a déclaré M. Grüniger.

Une excellente connectivité du système de santé

L'entreprise, basée à Root/LU contribue avec ses 95 collaborateurs de manière significative à l'efficacité, à la sécurité et à la connectivité du système de santé: 100 % des caisses maladie (LAMal/assurances complémentaires), 99 % des caisses accidents, 98 % des pharmacies, 95 % des hôpitaux, 81 % des laboratoires et les 26 cantons font désormais partie du réseau MediData. Environ 8700 médecins, plus de 760 organismes de soins à domicile et plus de 1100 maisons de retraite et établissements médico-sociaux utilisent également le réseau MediData. En 2024, 105.8 millions de documents électroniques ont été transmis. Le chiffre d'affaires s'est élevé à 39.263 millions de francs.

Continuité au conseil d'administration

Lors de l'assemblée générale annuelle, les actionnaires ont approuvé toutes les propositions du conseil d'administration: notamment le rapport de gestion et les comptes annuels 2024 ainsi que l'affectation des bénéfices et des réserves et ils ont donné décharge aux membres du conseil d'administration et de la direction. KPMG SA, Lucerne, a été confirmée à l'unanimité comme organe de révision pour l'exercice 2025. Anne-Geneviève Bütikofer, Andreas Dummermuth et Benno Fuchs ont été réélus membres du conseil d'administration pour un nouveau mandat de trois ans.

La sécurité, source de confiance

«En 2024, le volume de transport a franchi pour la première fois la barre des millions de passagers, dépassant les 20 000 liaisons», a souligné Daniel Ebner, CEO. «Pour nous, il ne s'agit pas seulement de chiffres. La sécurité est le fondement de la confiance, et la confiance est la base d'une santé numérique efficace. Avec la certification ISO 27001 et la certification de pro-

La cybersécurité est plus importante que jamais. Les criminels accèdent à des données précieuses avec une précision et une sophistication toujours plus grandes. La prévention est devenue essentielle.

Ernesto Hartmann d'InfoGuard a fait sensation avec sa présentation: Des forces obscures s'affairent à voler des données, et malheureusement, elles y parviennent avec succès.

tection des données selon l'Office fédéral de la santé (VDSZ), nous établissons des normes en matière de traitement des données de santé. Nous développons continuellement nos solutions, non pas pour elles-mêmes, mais parce qu'un système de santé en réseau fiable profite à tous les acteurs et améliore, par conséquent, la qualité de vie en Suisse.»

Les données sont précieuses et tentantes

Non seulement les changements structurels du système de santé progressent rapidement, mais les volumes de données à utiliser et à archiver en toute sécurité augmentent également à une vitesse fulgurante. Parallèlement, les prestataires de soins fusionnent et se mettent en réseau. Les processus administratifs et médicaux se complexifient, et avec l'intelligence artificielle et la médecine personnalisée, d'énormes sources de nouvelles données se multiplient.

Donc il n'est pas étonnant que ces précieuses données suscitent également l'intérêt de personnalités obscures. Ernesto Hartmann, responsable de la cyberdéfense chez InfoGuard, entreprise suisse et leader du marché de la cybersécurité, a démontré la menace que représente ce scénario. La cybercriminalité est devenue un véritable fléau. Le modèle économique est en plein essor et prospère sans complexe. Avec un chiffre d'affaires mondial de 9500 billions de dollars, ce secteur obscur est devenu la troisième plus grande «économie nationale»; seuls la Chine, avec 17 900 billions et les États-Unis, avec 27 900 billions de dollars, sont plus puissants. Comme prévu, les attaques informatiques n'arrêtent pas devant les portes des entreprises et institutions suisses. Les chiffres impressionnants de l'équipe d'intervention en cas d'incident de sécurité informatique (Computer Security Incident Response Team, CSIRT) d'InfoGuard le démontrent: «Le nombre élevé de cas signalés par le Centre des opérations de sécurité (SOC) et le CSIRT nous permet de disposer d'informations actualisées sur la situation des menaces», a déclaré Ernesto Hartmann. «En 2023, on a recensé 260 incidents en Suisse, 264 en 2024, et déjà 137 au cours des quatre premiers mois de 2025, et ce nombre est en augmentation. Chaque cyberattaque est un avertissement; nous devons agir et en tirer des leçons.»

Des attaquants plus sophistiqués menacent de plus en plus les petites entreprises

Ce conseil est essentiel, car les attaquants sont de plus en plus sophistiqués et organisés. Ils obtiennent non seulement des données potentiellement intéressantes via le dark web, mais gèrent également eux-mêmes des systèmes d'accès initiaux et des centres de développement lourdement financés. Malheureusement, les pirates informatiques connaissent un franc succès et ciblent de plus en plus les petites entreprises qui, d'après expérience d'InfoGuard, ont mis en place une protection informatique moins sophistiquée. Cela a été particulièrement vrai en 2024. Les entreprises concernées, en particulier celles de plus petite taille, souvent contraintes de payer des rançons en raison de sauvegardes détruites, ont transféré pendant l'année dernière 2.2 millions de dollars aux criminels. Cela correspond à 28 % du total des sommes réclamées, contre seulement 18 % en 2023.

Malheureusement, la tendance se poursuit. De janvier à fin avril 2025, 26 incidents de rançongiciel ont été traités par l'équipe CSIRT d'InfoGuard. Une rançon de 3.8 millions de dollars a déjà été versée. La plus grande surface d'attaque permettant aux criminels d'accéder aux bases de données a été fournie par ceux qui cherchaient à usurper l'identité. Les e-mails d'hameçonnage demeurent une source majeure de danger. Ernsto Hartmann a rapporté un cas très grave: un e-mail d'hameçonnage contenait un lien hypertexte vers un site web compromis, conçu pour espionner les identifiants Microsoft 365 et voler les cookies de session. Grâce au contournement de l'authentification et de l'authentification multifacteur (AMF), il a été possible de contourner le cookie de session volé et le processus d'authentification, même si les utilisateurs avaient activé une authentification multifacteur (AMF). Les mesures de sécurité telles que l'AMF sont ainsi compromises et les accès non autorisés deviennent possibles.

Prévenir efficacement des dommages considérables

Une lueur d'espoir pourrait provenir du fait que les voleurs de données professionnels ont adopté certaines règles «éthiques». Il s'agit notamment de s'abstenir d'attaques contre les données dans certains pays, principalement dans les pays d'Europe de l'Est, ou de faire preuve de considération envers les organisations à but non lucratif ou les infrastructures hospitalières essentielles à la vie. Cependant, on

Dans le secteur de la santé, le flux de données augmente rapidement, tout comme l'interconnexion et la complexité des processus. Tout cela nécessite une prévention complète en matière de sécurité.

Daniel Ebner, CEO, et le Dr German Grüniger, président du conseil d'administration de MediData, se réjouissent de la croissance réalisée, du financement solide et de la mise en œuvre réussie de projets innovants

ne peut pas toujours compter sur ces principes. La prévention reste précieuse, car même une interruption de courte durée des activités d'un hôpital peut être dévastatrice, engendrer des coûts très élevés et nuire gravement à sa réputation. Ernesto Hartmann a décrit des hôpitaux qui ont dû passer à des systèmes papier pendant plusieurs jours et qui, après avoir résolu la crise des pirates informatiques, ont dû redémarrer leurs systèmes au prix d'énormes efforts.

En conclusion, l'expert a déclaré: «En informatique, nous disposons d'un accès privilégié aux systèmes et aux données critiques. Il est de notre devoir de gérer ces ressources de manière sûre et responsable.» C'est la mission des 90 spécialistes d'InfoGuard pour plus de 400 clients.

La sécurité – partie intégrante de l'ADN de MediData

MediData, soutenu par InfoGuard, accorde depuis longtemps une attention particulière à la cybersécurité. L'une des mesures les plus importantes consiste à garantir que seul le personnel autorisé puisse accéder aux données sensibles des clients. Au sein du réseau MediData, les applications individuelles, notamment le portail client, où les utilisateurs peuvent configurer leurs paramètres, et l'outil interne du service d'assistance, sont entièrement protégées. L'authentification des utilisateurs est assurée par un certificat contenant une paire de clés, tandis que l'accès est accordé via un code d'accès renouvelé automatiquement. La solution choisie permet d'attribuer différents rôles aux utilisateurs de plusieurs unités.

L'infrastructure informatique et l'organisation de MediData sont également soumises aux exigences de sécurité les plus strictes. Elles sont continuellement mises à jour et certifiées ; des audits ISO 27001:2022 et VDSZ:2023 ont récemment été réalisés avec succès.

La sécurité informatique reste un enjeu majeur pour l'avenir. Par ailleurs, comme l'a expliqué Bernhard Joos, CIO, lors de l'assemblée générale, l'entreprise continuera de promouvoir la numérisation du système de santé dans les années à venir: «Afin d'identifier en amont les dernières évolutions et les besoins du marché, nous avons créé un outil spécial, le trend radar. Le développement du réseau MediData est un axe important pour l'avenir. En 2024, de nombreux éditeurs de logiciels et leurs clients ont adopté le nouveau service web. Cette transition sera achevée en 2025, permettant à tous les prestataires de services d'accéder au réseau MediData directement depuis le logiciel de l'hôpital ou du cabinet, grâce à un certificat et sans matériel physique supplémentaire.

Nous investissons également dans le développement de nos solutions tarifaires afin de garantir à nos partenaires une base solide et durable pour l'audit des prestations. Nous soutenons la transition vers la norme de facturation XML 5.0 du Forum d'échange de données afin de rendre la communication et la facturation électroniques au sein du système de santé encore plus efficaces et transparentes. Cela concerne les nouveaux tarifs des médecins ambulatoires (TARCOD et forfaits ambulatoires) ainsi que l'élargissement du contenu, au bénéfice de tous les acteurs du secteur de la santé suisse.

Le portail patients a été lancé avec plein de succès en avril 2022 et est largement utilisé. À ce jour, plus de 26 millions de factures ont été transmises en toute sécurité. Le portail patients continue de connaître une forte croissance: le nombre de transactions a augmenté de près de 27 % par rapport à la même période l'année dernière. Enfin, nous nous engageons en faveur de l'interopérabilité et invitons tous les partenaires du système de santé à développer conjointement des solutions qui renforcent l'ensemble de l'écosystème.»

Informations complémentaires

www.medidata.ch