Eléments décisifs pour une meilleure sécurité des données dans le domaine de la santé publique

MediData: sûr et durable – un bon sentiment

Presque aucun autre domaine ne détient autant de données sensibles nécessitant le plus haut degré de protection de la personnalité que celui de la santé publique. Par ailleurs, la loi de Moore, selon laquelle le volume des données double tous les 18 mois se fait ressentir ici fortement. Les procédés d'imagerie médicale innovants, l'interconnexion croissante des différents acteurs et, de manière plus générale, la numérisation grandissante engendrent des quantités astronomiques de données qui doivent de plus en plus être échangées en toute sécurité. Une sécurité sans compromis est indispensable. Nous avons demandé à MediData, dont les spécialistes sont au service du transfert de données, quels sont les défis qui en résultent.

«La sécurité chez MediData est en principe toujours une sécurité double», souligne Daniel Bätschmann, adjoint du CEO et responsable informatique. «D'une part, nous disposons à Root, notre siège social, d'une technologie de l'information qui se situe toujours à la pointe du progrès et qui répond aux plus hauts standards de sécurité. Cela concerne notamment l'accès aux données ainsi qu'une alimentation au courant et une climatisation sans interruption. D'autre part, nous disposons depuis août 2015 d'une colocation dans un centre de données de CKW Fiber (une filiale des Forces Motrices de la Suisse centrale CKW) dans laquelle l'ensemble des données existantes à Root sont mises en miroir sous des conditions tout aussi strictes. Le canton de Lucerne et l'hôpital cantonal de Lucerne ont également recours aux services de cet établissement performant. La connexion est assurée par des fibres optiques noires. Nous considérons cette double sécurité comme un élément décisif de notre business continuity management dans le cadre des certifications ISO 27001 / OCPD. Nous nous penchons sans cesse sur la question: quels scénarios pourraient se produire? Dans un cas extrême, combien de temps serait-il envisageable de ne pas pouvoir accéder aux données?»

Daniel Bätschmann, adjoint du CEO et responsable informatique

Le plus haut niveau de sécurité dès le départ

Avant qu'un stockage des données soit aménagé sur un autre site avec la colocation, une deuxième salle des serveurs existait déjà à Root. «Les deux salles», déclare Daniel Bätschmann, «ont naturellement offert dès le départ une protection hors pair contre les pannes de courant, les incendies et les inondations. Cependant, en raison de notre croissance, nous étions désireux d'aller encore plus loin. Même si les deux salles de serveurs existantes devaient tomber en panne simultanément, nous pourrions revenir en ligne en un rien de temps grâce à la colocation. Nos clients peuvent s'y fier. Nous sommes parés pour l'avenir.»

La sécurité commence auprès des collaborateurs

Une technologie de l'information de pointe est une chose, le comportement des collaborateurs en est une autre. «Je considère cela comme étant la base essentielle, car le transfert de données sensibles du domaine de la santé publique, qui a énormément augmenté ces dernières années, requiert une sécurité sans faille à tous les niveaux. En matière de sécurité, notre

Anita de Jong, conceptrice de logiciels et préposée à la sécurité

crédo est par conséquent: nous voulons gagner la confiance illimitée de nos clients, les fournisseurs de prestations dans les hôpitaux, cabinets, pharmacies et laboratoires, et bien sûr aussi les patients dont ils s'occupent. Tous devraient être sûrs à chacun instant que jamais rien n'arrivera à leurs données. Des accès frauduleux et illicites ne doivent pas se produire. Avec notre procédure PKI, nous veillons ainsi dans tous les cas à ce que l'expéditeur et le destinataire de données soient bien les bons.

Nos collaborateurs savent qu'il est primordial que notre activité soit fiable à cent pour cent. L'intégrité de nos spécialistes est tout aussi importante que la sécurité technique. Nous nous considérons aussi comme les administrateurs de nos clients dans notre tâche quotidienne.»

Formation au fur et à mesure, information et formations continues

A leur arrivée dans l'entreprise, puis régulièrement en cours d'embauche, tous les collaborateurs sont formés en matière de sécurité de l'information et de protection des données. «Chez nous, la sécurité est un thème récurrent avec de nombreuses facettes. Nous souhaitons que nos clients ressentent à chaque contact avec nos collaborateurs que chez nous, un climat de sécurité règne sans réserve», souligne Daniel Bätschmann. «Cette philosophie d'entreprise est valable pour tout le monde, même s'il n'y a que très peu de collaborateurs qui ont un accès direct à nos systèmes informatiques. Nous nous employons fortement à ce que nos collaborateurs soient motivés à participer activement pour tout ce qui relève de la sécurité. Cela implique de comprendre ces aspects, de les accepter et de savoir qu'ils sont utiles à tous. L'ensemble des thèmes qui s'y rattachent est transmis à chacun selon son niveau et sa fonction. Si des modifications sont effectuées dans le paysage sécuritaire et dans les documents concernés, elles sont communiquées immédiatement, tout comme les menaces imminentes telles que les cyberattaques peuvent en représenter. Une newsletter interne qui paraît mensuellement constitue le dernier maillon de la

chaîne de circulation des informations. Toutes ces mesures en faveur de nos collaborateurs représentent à nos yeux un investissement particulièrement important.»

Confiance et intégrité pour protéger les clients

Les clients de MediData peuvent suivre toutes les transactions. Ils bénéficient ainsi d'une transparence complète pour chaque flux de données. «Nous, par contre, n'avons pas accès aux données personnelles particulièrement sensibles», explique Daniel Bätschmann.

Un autre service est d'importance majeure. Bon nombre de cabinets facturent leurs prestations selon le système du tiers garant par le biais de MediData. Avec ce système, les factures des prestations doivent être envoyées aux patients rapidement, la plupart du temps par voie postale. Un service d'impression et d'étiquetage conduit directement à une installation d'emballage pour aller ensuite immédiatement au service d'expédition.

Pour le responsable informatique, une chose est claire: «Nous voulons savoir à tout moment où les données se trouvent. Nous remplissons ainsi notre devoir de diligence envers nos clients. Ceux-ci peuvent compter sur un échange simple, sûr et inaltéré des données. Ce sont justement les processus clairs et transparents qui simplifient la collaboration et ajoutent de cette manière une dimension supplémentaire à la sécurité. Les données des clients doivent toujours être à leur disposition, de jour comme de nuit. Toute utilisation des données par des tiers doit être exclue, tant sur le plan organisationnel que technique. Le respect des critères de sécurité et de qualité est évalué annuellement lors d'audits de maintien et tous les trois ans lors d'un processus approfondi de renouvellement des certifications. À noter: chez nous, la certification ne concerne pas uniquement des processus isolés, mais l'entreprise dans son ensemble.»

Un développement sûr et autonome

Et comment les évolutions informatiques se déroulent-elles compte tenu de la croissance florissante de MediData? – Cette tâche est assumée par trois équipes qui conçoivent tout ce qui est spécifique à l'entreprise. «Là aussi, nous prenons la protection des données très au sérieux à chaque étape. Par exemple, nous nous offrons le luxe de fabriquer des données de test totalement synthétiques plutôt que de nous contenter de les tirer de données productives.

En informatique à proprement parler, l'élimination est un sujet très délicat. Bien que les données soient cryptées sur les supports de données, nous apportons un soin particulier à ce que les pièces défectueuses ou mises au rebut soient détruites en bonne et due forme. Tout compromis en la matière est exclu», souligne Daniel Bätschmann.

Il ne faut pas oublier non plus la dimension sécurité Internet. «Cela constitue souvent un domaine complexe pour nos clients», admet notre interlocuteur, «ici, nous faisons tout pour rester en contact étroit avec nos 8000 partenaires de contrat et soutenir efficacement les

Jouer la sécurité: toutes les données générées ici à Root sont aussi mises en miroir dans la colocation avec un soin minutieux.

petits prestataires en particulier, afin d'éviter que des risques ou des fuites d'informations apparaissent chez eux.»

Bien organisé – bien protégé

Anita de Jong, conceptrice de logiciels et préposée à la sécurité, partage l'avis du responsable informatique: «La sécurité commence avec chacun de nous. Et pour cela, il faut l'organisation nécessaire.» – La commission de sécurité interne est constituée des trois membres de la direction ainsi que de notre interlocutrice et forme une base solide. La commission est responsable de la stratégie de sécurité. Les directives y sont définies et appliquées top down (de haut en bas) au sein de l'entreprise. Au quotidien, le noyau de l'équipe de sécurité, c.-à-d. Daniel Bätschmann et Anita de Jong, a les rênes en main, il sonde et planifie toutes les tâches soigneusement, et fixe les priorités. «Faire ce qu'il faut à temps, telle est la devise. Outre le transfert de données avec les clients, cela concerne également le système de gestion numérique propre à l'entreprise et la documentation des données concernées, qui relèvent par exemple de la finance et de la comptabilité.»

La commission se réunit régulièrement. Elle examine alors avec soin où en sont tous les projets d'informatique et de sécurité, si les équipes progressent bien dans leur travail, si de nouvelles priorités sont rendues nécessaires en raison d'évolutions techniques ou de la croissance de l'entreprise, si des prestations doivent être étendues afin de garantir une haute performance, et pour finir, la commission examine les influences extérieures sur MediData. De nouvelles impulsions peuvent être données par des réglementations, des exigences des clients ou de nouvelles solutions en matière de cybersanté (eHealth).

Durabilité et objectifs de sécurité bien définis

L'état des lieux en profondeur qui est régulièrement effectué se penche sur les nombreuses facettes de la sécurité de l'information telles que la confidentialité, l'intégrité ainsi que la grande disponibilité des informations, des données et des systèmes. La protection des données à proprement parler, appliquée dans le respect des prescriptions légales, est tout aussi importante. «Nous voulons continuellement améliorer l'efficacité de la sécurité informatique par le biais de planifications, de mises en œuvre et de contrôles conséquents et, là où c'est nécessaire, de rectifications. Dans ce but, nous avons recours à des audits internes et externes, tout comme à des analyses de risques, des vérifications de mesures, des contrôles d'enregistrements et des évaluations d'incidents de sécurité, à intervalles réguliers.»

Des directives-cadres tout aussi strictes s'appliquent pour le domaine de la protection des données. L'ensemble des processus et des mesures requis pour l'aménagement, la mise en œuvre, l'application, la surveillance, le contrôle, la maintenance et l'amélioration continue doit être établi et exploité de manière optimale.

«Une sécurité sans compromis, qui transparait en particulier dans la mise en place de la colocation, ainsi que des contrôles permanents restent la priorité première. En même temps, nous veillons à ce qu'il soit bien défini qui remplace qui parmi les collaborateurs, les connaissances doivent rester dans l'entreprise, les formations continues permettent de renforcer cet effet. Et cela crée les conditions optimales pour garantir constance et durabilité, car la sécurité est un thème récurrent et il le restera toujours chez nous», Daniel Bätschmann comme Anita de Jong s'y fient.

Texte: Dr Hans Balmer

MediData – pour une évolution saine dans le domaine de la santé publique suisse

MediData est un prestataire informatique déterminant dans le domaine des services électroniques de la santé en Suisse et dans les régions limitrophes. Les 62 spécialistes de notre entreprise servent de trait d'union entre les prestataires (médecins, pharmacies, hôpitaux, laboratoires, établissements médico-sociaux, services d'aide et de soins à domicile, etc.), les assureurs-maladie et accidents, les cantons et les patients grâce à des solutions informatiques efficaces. L'objectif consiste clairement à interconnecter tous les acteurs du secteur de la santé suisse, et à garantir ainsi un échange efficace des informations ainsi que des processus optimaux.

Les clients et partenaires apprécient spécialement chez MediData
– **la sécurité** (certifiée conformément à la norme ISO 27001 et à l'ordonnance OCPD)
– **l'expérience** (établie depuis plus de 20 ans dans le domaine de la santé publique suisse)
– **la qualité** (valeurs durables: respect, loyauté, clarté, fiabilité et gestion d'entreprise)
– **l'aide apportée** (suivi individuel – l'individu est au cœur de nos préoccupations)
– **le savoir-faire** (grande compétence et expérience grâce à des spécialistes travaillant déjà depuis dix ans ou plus chez MediData)