

Enjeux et challenges des services cloud

Numérisation Les services de stockage cloud permettent de réduire les efforts et les coûts informatiques. Mais qu'en est-il de la protection et de la sécurité des données? Comment les professionnels de la santé peuvent-ils s'assurer de la protection des données sensibles?

Torsten Kahlstadt

Vous arrive-t-il de stocker vos documents personnels sur Google Drive, OneDrive, Dropbox, iCloud ou autre? Certes, stocker des données sous cette forme présente de nombreux avantages. On peut, par exemple, accéder à ses informations quel que soit le lieu et depuis n'importe quel appareil, aucun autre matériel n'est nécessaire et finies les sauvegardes manuelles! Sans surprise, les solutions cloud s'imposent de plus en plus dans le milieu professionnel.

Des données de santé dans le cloud?

La loi sur la protection des données considère les informations relatives à la santé comme particulièrement sensibles, nul besoin de vous l'expliquer à vous, professionnels de la santé. Par conséquent, il faut soigneusement protéger ces données contre toute utilisation abusive et contre l'accès par des tiers. Cela vaut également pour le stockage ou l'échange de données via un cloud. Ce n'est ni mauvais ni interdit. Toutefois, il est indispensable d'examiner minutieusement les différentes solutions cloud et les éventuels risques avant utilisation. En effet, déléguer les responsabilités, un des avantages du cloud, rime malheureusement avec perte de contrôle. En plaçant des données dans un cloud, il est difficile de contrôler ce qui se passe ensuite: où sont-elles stockées? Qui peut les consulter et les traiter?

Garantir la sécurité des données

Le stockage des données sensibles doit respecter trois points fondamentaux: les données doivent être protégées contre le vol, le traitement non autorisé et les fuites; elles doivent être sécurisées contre les accès non autorisés et les cyberattaques; enfin, les exigences légales et d'autres réglementations en vigueur doivent être respectées. Les solutions de «cloud computing» dans le secteur de la santé doivent en tenir compte. Ainsi, une multitude de critères entrent en jeu pour choisir le service cloud adapté. En voici quelques exemples: le fournisseur doit utiliser un bon pare-feu pour les applications web, effectuer des sauvegardes régulières et disposer d'une gestion des accès bien pensée et assortie des restrictions appropriées.

Attention aux certifications

Vérifier et comparer un catalogue de critères pour différents prestataires s'avère complexe et onéreux. Pour se faire une

idée de la qualité et du sérieux d'un fournisseur, les certifications sont, à mon avis, révélatrices. Vérifiez si les politiques et procédures de sécurité du fournisseur reposent sur des normes de sécurité généralement reconnues comme la norme ISO 27001 ou le NIST (National Institute of Standards and Technology). Si tel est le cas, le niveau de sécurité est déjà bon. De plus, je vous recommande de lui demander s'il tient compte des exigences de la loi sur la protection des données (LPD), des dispositions d'exécution inscrites dans l'ordonnance sur la protection des données (OPD) et du règlement général sur la protection des données (RGPD).

Autres pays, autres mœurs

Tous les pays n'accordent pas la même importance à la protection et à la sécurité des données. Aux États-Unis, par exemple, le Patriot Act et la loi FISA (Foreign Intelligence Surveillance Act) rendent la garantie d'une protection des données conforme aux exigences européennes ardue. Les entreprises, y compris les fournisseurs de services cloud, sont soumis à la juridiction du pays de leur siège social. Si vous ne voulez pas passer en revue les directives de protection des données des autres pays, je vous recommande d'utiliser la solution de stockage d'un fournisseur suisse, qui permet de conserver en tout temps vos données dans votre pays.

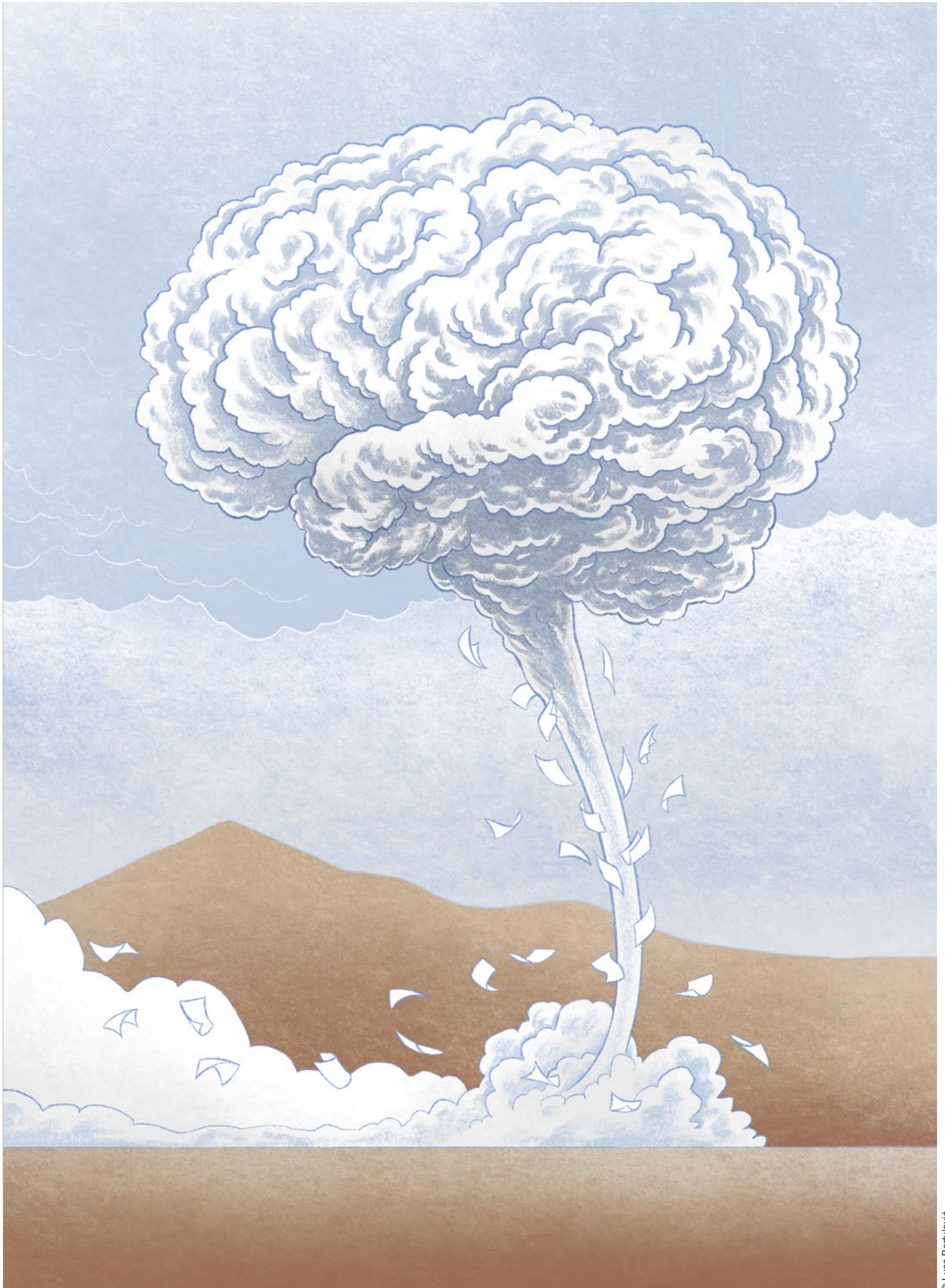
Prudence est mère de sûreté

Ce qui vaut pour la protection et la sécurité des données est vrai pour le stockage dans le cloud: la prudence est essentielle. Utiliser des solutions gratuites sans vérifier au préalable ce qui se passe avec les données téléchargées n'est assurément pas une bonne idée. Restez conscient de la sensibilité des données de santé et choisissez votre solution cloud avec soin. Si vous n'êtes pas sûr de vous, un spécialiste en informatique peut vous aider.



Lucas Schult

est directeur (CEO) de HIN. Il écrit régulièrement dans cette rubrique à propos de la sécurité numérique.



© Luca Bartulović