Se prémunir contre la fuite de données

Protéger les données des organisations est un chantier permanent qui nécessite la mise en place d'outils informatiques, de procédures bien cadrées, ainsi que des efforts de formation des personnels aux risques encourus. Des niveaux d'intervention complémentaires, sinon indissociables.

Les organisations du secteur social et médico-social traitent de nombreuses informations personnelles. Selon le règlement général sur la protection des données (RGPD) notamment, elles sont dans l'obligation d'en assurer la sécurité et d'en restreindre l'accès à des professionnels habilités. Il en va de même pour celles qui sont sensibles (comptables, financières, etc.). Toutes ces données doivent être protégées d'un acte de piratage informatique aux conséquences parfois désastreuses. « *Les structures comprennent les enjeux d'une fuite de données mais c'est un risque auquel elles sont plus ou moins sensibilisées,* indique Philippe Passis, directeur du groupement social de moyens Ressourcial. *Beaucoup d'entre elles pensent ne pas être concernées, s'estimant trop petites ou sans intérêt pour être la cible d'une cyberattaque.* » Une erreur : s'il y a des piratages qui visent les grandes organisations, potentiellement riches aux yeux des hackers, il y en a aussi des non ciblées. Il est donc indispensable que toutes se protègent. Ce qui nécessite de travailler sur deux axes principaux.

1 Des protections numériques

Le premier est d'ordre technique : activation d'un pare-feu, déploiement d'un antivirus, mises à jour et sauvegardes régulières des matériels et logiciels, sécurisation de la messagerie… « *Nous sommes en retard à ce niveau, et plus globalement à celui des systèmes d'information. Même si le secteur avance vite ces dernières années, il accuse une dette technique assez forte par rapport à l'état de l'art ou même par rapport au secteur sanitaire* », commente Philippe Passis. Il est donc urgent d'y consacrer des ressources financières et humaines. Ce qu'a fait Hovia, association gérant une soixantaine d'établissements et services. « *Outre la mise en place d'antivirus, de pare-feu, etc., nous avons également amélioré depuis 2017 nos procédures internes concernant l'accès aux systèmes. Nous avons, par exemple, clôturer des comptes de personnes ne faisant plus partie des effectifs* », détaille Baptiste Foulon, directeur de l'Offre et de l'Innovation.

© Irsam

Un des process à suivre selon Nadège Vanneste (Irsam) ? Utiliser des mots de passe complexes.

2 Une sensibilisation indispensable

Les meilleures barricades technologiques ne servent à rien si un salarié laisse une porte grande ouverte. Le second axe sur lequel il faut travailler est la sensibilisation des personnels au risque de fuites. « *Nous communiquons en ce sens auprès de nos salariés* », explique Nadège Vanneste, directrice des services de l'information et de l'organisation à l'association Irsam employant environ un millier de personnes. « *En 2023, nous mettons en place une politique de sécurité plus structurée avec un plan de communication précis. La première campagne a pour thème l'utilisation de mots de passe plus complexes.* » Le choix de sésames difficiles à deviner semble une évidence. Il est toutefois indispensable de le rappeler. « *Depuis la crise sanitaire, il y a plus de collaborateurs qui télétravaillent. Nous avons dû leur rappeler qu'il ne fallait pas envoyer de données sensibles par mail non protégé* », insiste Nadège Vanneste. Pour avoir le meilleur impact possible, chez Hovia, la communication passe aussi par le terrain. « *Nous faisons porter les messages sur les bons usages et la sécurité par les directeurs et les correspondants informatiques dans les établissements,* précise Baptiste Foulon. *Ils ont souvent une plus grande portée auprès des salariés du fait que cela vient de leurs collègues plutôt que du siège.* »

« Ne pas envoyer de données sensibles par mail non protégé. »

Reste que ces messages doivent être réitérés sans cesse ; tout comme les mesures techniques doivent être actualisées pour rester protectrices. La prévention de la fuite de données, plus globalement la sécurité des systèmes d'information, est un travail de Sisyphe.

Pascal Nguyên

POINT DE VUE

© Hovia

Baptiste Foulon, directeur de l'Offre et de l'Innovation chez Hovia, à Paris

« En 2017, nous avons fait réaliser un audit de sécurité de nos systèmes d'information par le service numérique de santé (Sesan), un groupement d'intérêt public spécialisé en solutions numériques en Île-de-France. Cela nous a permis d'identifier les mesures d'amélioration, que nous mettons en œuvre depuis. Cependant, de nouvelles failles peuvent apparaître. D'ailleurs, pour les identifier, nous commandons à un prestataire des tests d'intrusion et de vulnérabilité tous les deux ou trois ans. Cela représenterait un coût de 20000 à 30000 euros que nous épargne le mécénat de la société de sécurité qui les réalise. Par ailleurs, les actions de sensibilisation des personnels doivent également être reconduites régulièrement du fait du *turn-over* et des bonnes habitudes qui se perdent avec le temps. La sécurité des données est un chantier sans fin. Il faut en avoir conscience. »

RESSOURCES

- **Guide de cybersécurité destiné au secteur médico-social de l'ANS sur https://esante.gouv.fr**