© FOTOLIA

DONNÉES DE VOS PATIENTS

Se prémunir contre la cybercriminalité

Les attaques cybercriminelles ne cessent d'augmenter et représentent un risque majeur pour les biologistes dont l'une des principales responsabilités est précisément de protéger les données de leurs patients. Face à ces risques croissants, ils doivent donc anticiper, y compris sur le plan assurantiel.

L'essor d'Internet et son utilisation croissante dans le cadre du développement de l'activité économique ainsi que le stockage de données vont de pair avec l'augmentation de la cybercriminalité. Un phénomène caractérisé par des actes malveillants à l'encontre d'un dispositif informatique tel que les systèmes d'information des laboratoires, via un réseau cybernétique. Les cyberattaques pourraient même entraîner jusqu'à 400 milliards de dollars de pertes par an dans le monde, selon une étude réalisée en juin dernier par l'éditeur de solutions de sécurité McAfee. Un rapport qui indique par ailleurs que ce chiffre est probablement loin de la réalité, la plupart des actes de cybercriminalité n'étant pas signalés par les entreprises qui en sont victimes. En outre, la collecte de données cohérentes sur le sujet demeure difficile à effectuer en raison du flou autour du terme cybercriminalité.

Les biologistes médicaux n'échappent pas aux risquent de se faire « hacker » leurs systèmes informatiques, explique Christophe Choumil, courtier d'assurances spécialisé dans le secteur : *« Il en existe aujourd'hui deux types principaux : le vol de données et le détournement de téléphone portable. »* Destruction de données, tentative d'extorsion, usurpation d'identité, utilisation frauduleuse de la Carte vitale, volonté de nuire à la réputation d'autrui, prise de contrôle d'une entreprise, détournement de médicaments… : si les objectifs des hackers peuvent paraître flous, les conséquences sont quant à elles très graves. Or, rappelle Christophe Choumil, *« lorsque vous détenez des informations sur des tiers, vous avez l'obligation de tout mettre en œuvre pour les protéger et d'informer ces tiers en cas de vol, de manière à ce qu'ils aient la possibilité de prévenir les détournements éventuels »*.

Riposte de l'Union européenne

Pour contrer ce phénomène croissant, un nouveau règlement européen rendant systématiquement obligatoire la notification des atteintes aux données per- ...

... sonnelles et renforçant les sanctions applicables aux attaques devrait être transposé en France l'an prochain. Pour autant, il est plus sécurisant de se protéger individuellement, notamment en vérifiant le niveau de sécurité informatique de son laboratoire mais aussi en contractant une assurance contre la cybercriminalité. « *L'objectif d'une telle assurance est d'anticiper d'éventuels sinistres*, précise Christophe Choumil. *Les cyber-risques sont déjà très développés dans d'autres professions, notamment intellectuelles, y compris celles réglementées comme les avocats et les notaires, lesquels sont donc très équipés. Mais les biologistes n'y sont, pour l'heure, que peu sensibilisés. Aujourd'hui, presque aucun d'entre eux n'est équipé.* »

La divulgation d'informations médicales confidentielles peut pourtant avoir de graves répercussions sur la réputation et la vie privée des patients et elle engage la responsabilité du biologiste médical censé protéger ces données.

« La question est de s'assurer ou de faire de l'auto-assurance, autrement dit d'être son propre assureur. »

Quelles démarches ?

Avant de souscrire une assurance et de protéger son réseau informatique, il convient d'abord de réaliser un audit de son exposition (type de système informatique) et de vérifier les assurances de responsabilité civile de son prestataire pour savoir, en cas de sinistre, à quel niveau de montant l'on peut être remboursé. Si le niveau de garantie qu'offre ce prestataire n'est pas convaincant, une assurance cybercriminalité permet d'assurer les données détenues portant sur des tiers. Celle-ci couvre l'ensemble des données, y compris les conséquences de la diffusion des données, comme les reconstitutions d'image, les dommages et intérêts sur réclamation des tiers, la remise en état du système informatique ou encore la mise en place de protection.

Il s'agit donc de se protéger puis de s'assurer ou de s'auto-assurer pour le risque résiduel. Il faut comprendre qu'aucune mesure technique de protection n'est fiable à 100 %. « *Il n'y a pas d'obligation à s'assurer,* relève Christophe Choumil. *Mais la question est de choisir entre s'assurer ou de faire de l'auto-assurance, autrement dit d'être son propre assureur.* » ■