PROFESSION
>Maîtrise médicalisée des volumes.
L'indispensable mesure pour contenir les dépenses.

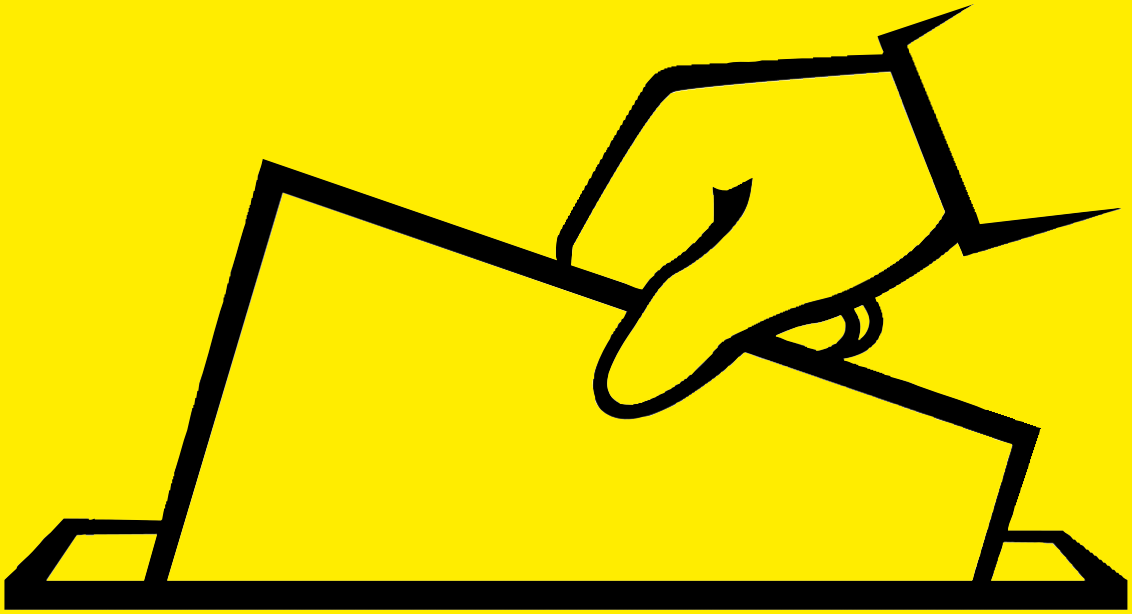
LABORATOIRE
>Cybersécurité.
Sécuriser les données des LMB.

EXPERTISE
>Recherche.
La porte s'ouvre pour les laboratoires de ville.

BiologieMédicale

N°115

le magazine du Syndicat des Biologistes



FOCUS

PRÉSIDENTIELLES

LE PROGRAMME DES CANDIDATS POUR LA BIOLOGIE MÉDICALE PRIVÉE

Trimestriel • Avril 2017 • 45€

CYBERSÉCURITÉ
Des portes blindées pour les données des LBM


© FOTOLIA

Longtemps ignorés, notamment dans le secteur de la santé, les cyber-incidents sont désormais une réalité pour l'ensemble des entreprises, y compris les laboratoires, d'autant plus que ces derniers connaissent actuellement une croissance exponentielle et qu'ils ne se pilotent plus sans de robustes systèmes informatiques. Au-delà du risque bien réel, les réglementations française et européenne obligeront les biologistes, dans les mois à venir, à prendre très rapidement des mesures pour se protéger.

En 2015, la France est passée dans le top 10 des pays les plus touchés par les cyber-attaques[1]. La même année, on comptait 21 incidents de cybersécurité par jour, pour un coût total estimé en France à 3,36 milliards d'euros. Et ce risque ne cesse d'augmenter : en 2016, plus de 80 % des structures françaises ont subi au moins une cyber-attaque dans l'année[2]. Les chiffres suffisent à convaincre les plus réticents que le sujet est désormais une réalité qui n'épargne malheureusement pas les laboratoires. Qu'elles soient directes ou indirectes, les conséquences sont graves et préjudiciables : retard ou arrêt complet de la production, coût de restauration, gestion de crise, violation des données médicales personnelles ou bancaires… Et les frais associés sont multiples : frais d'experts juridiques et informatiques, coûts d'information de la patientèle et de mise en œuvre des mesures correctrices et réparatrices à l'égard des victimes.

Un contexte réglementaire renforcé

Au-delà du risque lui-même, la réglementation – française et européenne – imposera très prochainement aux entreprises d'agir, et particulièrement aux laboratoires. En effet, le Règlement général sur la protection des données (RGPD) ainsi que la directive relative à la protection des données à caractère personnel à des fins répressives ont été adoptés le 14 avril 2016 par le Parlement européen. Ces dispositions sont directement applicables dans tous les États membres et ceux-ci ont deux ans pour transposer les dispositions de la directive dans leur législation nationale.

Parallèlement à la mise en place de cette directive, le champ de la santé fait l'objet d'une attention toute particulière en France. En effet, dans un décret du 12 septembre 2016, la France a instauré un système de collecte des incidents survenus dans les systèmes d'information des laboratoires de biologie médicale, des établissements de santé et des cabinets de radiologie, de façon à alerter l'ensemble de ces professionnels en cas …

LES PROCHAINES ÉTAPES À COURT TERME

- Mettre en place une politique de protection des données ainsi qu'un plan de continuité d'activité et un plan de reprise d'activité en cas de cyber-attaque.
- S'assurer que les solutions mises en place répondent à l'état de l'art.
- S'entourer d'experts pour, en cas de suspicion d'attaque, évaluer correctement l'impact.
- Mettre en place le poste de délégué à la protection des données personnelles (DPO).

... de cyber-attaque. Ce décret sera applicable à compter du 1er octobre 2017.

Par ailleurs, la loi du 7 octobre 2016 pour une République numérique[3] anticipe certaines dispositions du RGPD, comme le renforcement de l'obligation d'information (qui est prévue par la loi Informatique et Libertés) ou le renforcement des pénalités en cas de non respect de la loi, pouvant aller jusqu'à 3 millions d'euros d'amende.

Une sécurité à anticiper

Le RGPD va donc se substituer à loi Informatique et Libertés. Les éditeurs de logiciels et de solutions seront obligés de revoir leur politique de protection de la donnée personnelle. En effet, en cas de divulgation de ces données, le RGPD pose comme principe la coresponsabilité laboratoires-éditeurs. La protection des données devra donc être intégrée par tous, laboratoires et fournisseurs, dès la conception d'un projet informatique, et la sécurité devra être assurée conformément à l'état de l'art (contrôle d'accès, administration, prévention contre les failles de sécurité, etc.). Les LBM devront mettre en place des garanties pour assurer la protection des données et apporter la preuve que le règlement sur leur protection est bien respecté. L'ensemble des actions de cette politique de protection des données devra en outre être bien documentée en vue de l'information des autorités de contrôle. Enfin, en cas de fuite de données, avérée ou supposée, les entreprises seront tenues, en France, de les notifier à l'autorité nationale de protection, à savoir la Commission Nationale de l'Informatique et des Libertés (Cnil).

Bref, au regard de toutes ces mesures, il est urgent pour les biologistes d'agir, d'autant que le non-respect de cette directive n'est pas sans conséquence. En cas de plainte d'un patient ou d'une action collective, si l'entreprise n'a pas mis en œuvre de moyens humains et matériels pour assurer la non diffusion des données personnelles, les autorités de régulation de tous les pays de l'Union européenne pourront la sanctionner d'une amende maximale de 20 000 millions d'euros. Toutes ces actions seront assurées et vérifiées par le délégué à la protection des données personnelles (DPO), une nouvelle fonction différente du directeur des systèmes d'information (DSI), qu'il faudra également assurer au sein des laboratoires. ■

1. Source : Cabinet d'audit et de conseil PwC.
2. Source : Club des experts de la sécurité de l'information et du numérique (Cesin).
3. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

LES LBM, DES CIBLES DE CHOIX ?

Les biologistes sont des cibles de choix pour les *ransomware*, ces logiciels malveillants qui peuvent être propagés via un mail piégé et dont l'objectif est de compromettre le plus de systèmes possibles, de récupérer les données et ensuite d'en monnayer la restitution – en monnaie virtuelle de préférence, comme le bitcoin – pour échapper à toute traçabilité. Début 2015, une cyber-attaque avait ciblé un laboratoire implanté dans les Bouches-du-Rhône. Les pirates avaient exigé une rançon de 20 000 euros en échange d'une non-diffusion de 40 000 identifiants (nom, prénom, login, mot de passe) ainsi que de « centaines » de bilans médicaux volés. Face au refus de payer opposé par le laboratoire, les informations de 15 352 patients avaient été diffusées sur Internet.

LE CONTEXTE RÉGLEMENTAIRE RÉSUMÉ

2010

L'**ARTICLE L. 5232-4** du Code de la santé publique oblige à déclarer les incidents mettant en cause les logiciels qui ne sont pas des dispositifs médicaux et qui sont utilisés par les LBM.

26 JANVIER 2016

LOI DE MODERNISATION DU SYSTÈME DE SANTÉ.
> L'**ARTICLE L. 1110-4-1** stipule que la conservation, les échanges et la transmission des données de santé doivent se faire conformément aux référentiels d'interopérabilité et de sécurité.
> L'**ARTICLE L. 1111-8** modifie les conditions pour être hébergeur de données médicales.
> L'**ARTICLE L. 1111-8-2** renforce la sécurité des systèmes d'information des établissements de santé et des organismes et services exerçant des activités de prévention, de diagnostic ou de soins, lesquels doivent signaler à l'ARS, sans délai, les incidents graves de sécurité des systèmes d'information.
> L'**ARTICLE L. 1111-14** relance le DMP et transmet son contrôle à la Cnamts.

14 AVRIL 2016

Adoption au Parlement européen du **RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES** (RGPD) ainsi que la directive relative à la protection des données à caractère personnel à des fins répressives.

L'ARRÊTÉ DU 10 JUIN 2016

FIXE LES RÈGLES DE SÉCURITÉ ET LES MODALITÉS DE DÉCLARATION des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Produits de santé » et pris en application des articles **R. 1332-41-1**, **R. 1332-41-2** et **R. 1332-41-10** du Code de la défense.

« ON AURAIT PU PRENDRE LE CONTRÔLE À DISTANCE DE **100 % DES LABORATOIRES TESTÉS !** »

Bruno Gauthier, membre du Bureau national du SDB, trésorier de la Société française d'Informatique de Laboratoire (SFIL) et fondateur d'une plateforme de gestion des cyber-risques en Bretagne.

Les biologistes sont-ils conscients des cyber-risques ?
Bruno Gauthier : Non. Pour sensibiliser les biologistes de notre région à ce phénomène, le Syndicat des Biologistes de Bretagne Pays-de-Loire auquel j'appartiens a lancé une campagne d'hameçonnage (ou *fishing*, technique utilisée par des fraudeurs pour usurper les identités) auprès de 500 biologistes, pour évaluer la maturité des LBM face à ces attaques. 80 % des biologistes avaient au moins cliqué sur un mail et 100 % des laboratoires auraient pu être contrôlés à distance.

Pourquoi les laboratoires doivent-ils se saisir de ce sujet ?
B.G. : Les LBM font face à un double risque : d'un côté, ils manipulent des données particulièrement sensibles. De l'autre, l'informatique est devenue une composante présente tout au long de la chaîne de traitement des examens biologiques (automates, outils de pilotage des plateaux techniques, identification du patient, prescription connectée, serveurs de résultats, etc.). Et ce, dans un contexte de concentration en multi-site nécessitant une mise en conformité plus que rigoureuse des systèmes d'information du laboratoire (Sil).

En quoi consiste la plateforme de cybersécurité que vous avez mis en place dans votre région ?
B.G. : Nous avons mis en place en janvier 2017 un système en trois modules pour accompagner les laboratoires dans la mise à niveau de leur sécurité. Le premier module consiste à former le personnel au cyber-risque via une plateforme d'e-learning permettant de les mettre en situation de cyber-attaque et d'expliquer comment réagir. Trois campagnes de *fishing* par an sont également prévues pour s'assurer que la formation porte ses fruits. Le deuxième module est une plateforme de gestion de crise, un numéro vert joignable 24h/24, capable d'effectuer un premier niveau de diagnostic mais aussi d'intervenir sur site. Le dernier module est un audit d'hygiène informatique, sur la base de la norme ISO 27001 qui balaye l'ensemble du système d'information de manière plus détaillée que la norme ISO 15189. Un plan d'action est ensuite proposé sur six, douze ou dix-huit mois en fonction de l'état de la sécurité informatique. Une assurance cyber-risque est également proposée, conditionnée à la note obtenue à l'audit. ■

L'AVIS DU SDB

QUI VA PAYER ?

Le risque est réel, les contraintes réglementaires peu contestables… Résultat : les laboratoires de biologie médicale doivent investir dans leur sécurité informatique et souscrire de nouvelles assurances spécifiques ou s'auto-assurer. Le tout à leur frais et dans un contexte de contraintes budgétaires et de baisses de tarifs en décalage complet avec la hausse des charges de nos structures. Le point de rupture entre l'augmentation continue des charges et des obligations supplémentaires (accréditation, cybersécurité…) et la baisse de rentabilité de nos structures s'approche dangereusement. Le SDB demande une prise en compte de l'ensemble de ces contraintes nouvelles dans la détermination des tarifs des examens de biologie médicale.

12 SEPTEMBRE 2016

Publication du **DÉCRET n° 2016-1214** d'application des incidents de sécurité dans les établissements de santé, les laboratoires et les cabinets de radiothérapie.

7 OCTOBRE 2016

LOI n° 2016-1321 POUR UNE RÉPUBLIQUE NUMÉRIQUE. Certaines dispositions anticipent le règlement européen sur la protection des données personnelles applicable en mai 2018. L'obligation d'information prévue par l'article 32 de la loi Informatique et Libertés est renforcée. Les responsables de traitements de données doivent désormais informer les personnes de la durée de conservation des données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.

14 OCTOBRE 2016

INSTRUCTION N°SG/DSSIS/2016/309 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») dans les établissements et services concernés.

12 JANVIER 2017

ORDONNANCE n°2017-29 relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel.