Juillet 2020
435

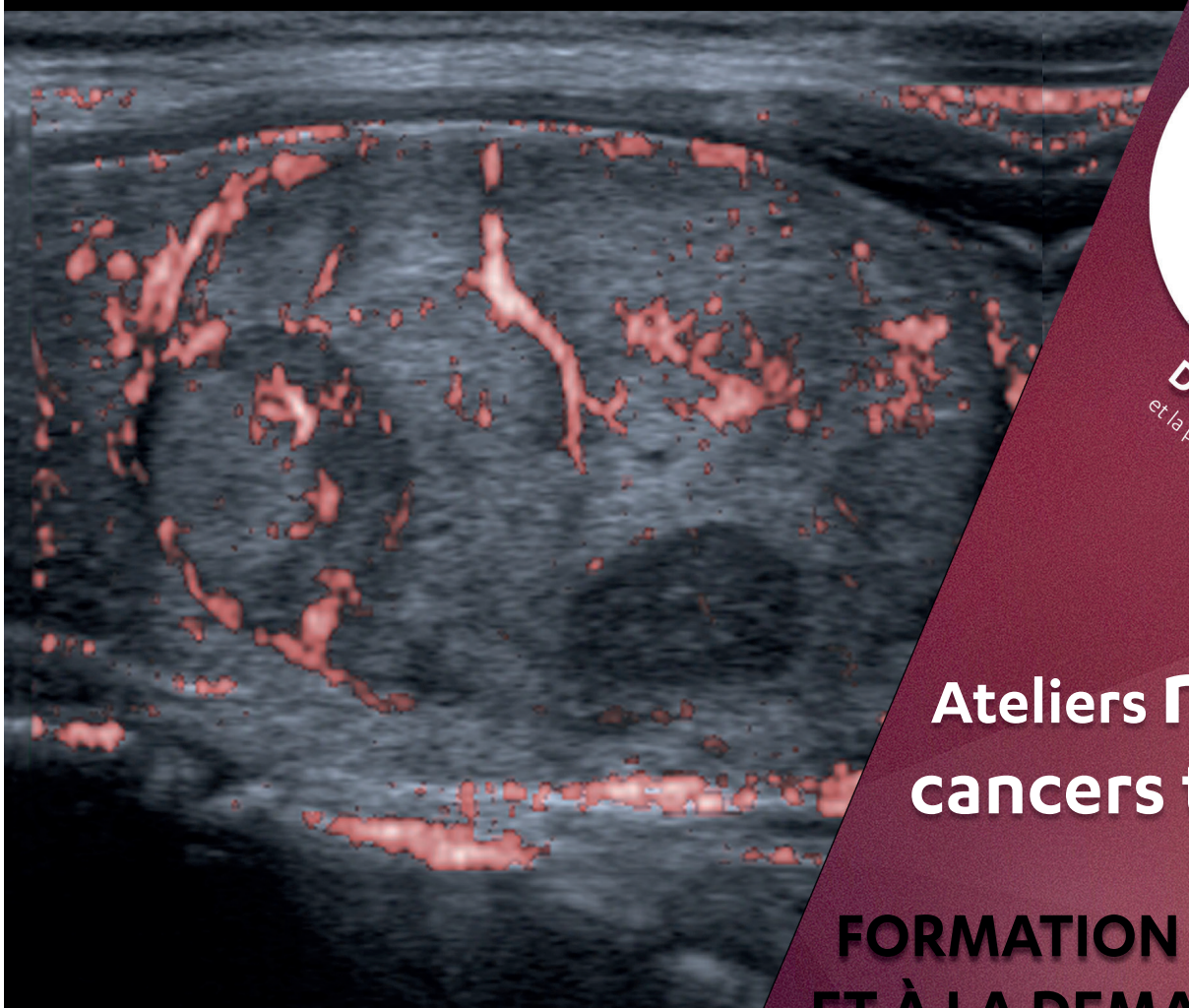
Le Médecin Radiologue de France

la lettre de la
FNMR Fédération Nationale des Médecins Radiologues

Cybersécurité

/LaFnmr
@Fnmr_radiologue
fnmr.org

FORCOMED



Dr Jean TRAMALLONI

et la participation du Dr Guillaume JOURDAN

Ateliers nodules et cancers thyroïdiens

FORMATION À DISTANCE ET À LA DEMANDE

1. Un parcours interactif avec 8 cas en pratique courante

2. Travailler les notions exposées lors de la formation « *Echographie des nodules et des cancers thyroïdiens* »

3. Travailler l'échographie des thyroïdites et des parathyroïdes

4. Travailler les difficultés dans l'élaboration du score EU-TIRADS

Frais d'inscription : 339€

Une nouvelle épidémie, informatique…


DR

Dr Jean-Philippe MASSON, Président de la FNMR

Le dernier séminaire de la FNMR, en janvier 2020, avait pour thème la **cybersécurité**.

L'ensemble de cette revue est donc consacré à **ce sujet qui devient de plus en plus important** pour tous les secteurs d'activité (l'Australie a été récemment attaquée violemment par des hackers) mais aussi spécifiquement dans le domaine de la santé et notamment les centres d'imagerie.

Les médecins radiologues doivent impérativement protéger leurs systèmes informatiques contre des intrusions malveillantes qui peuvent bloquer toute leur activité pendant de longues périodes. Le témoignage de l'un d'entre nous est très éloquent.

Bien sûr, la cybersécurité impose peut-être des réorganisations, des investissements mais ceux-ci seront réellement rentables.

Après la crise sanitaire que nous venons de passer, **les cabinets de radiologie n'ont pas besoin en plus d'être paralysés par des virus informatiques**.

L'activité semble reprendre dans nos centres et se rapprocher progressivement de ce qu'elle était avant l'épidémie mais cela ne suffira pas à compenser les pertes subies. Comme pour d'autres secteurs économiques en France, il faudra certainement attendre 2021 pour retrouver l'activité de 2019.

La rentrée de septembre donnera, espérons-le, des indications. Les grands événements radiologiques de la fin de l'année : les JFR seront-elles effectivement maintenues ? L'ECR, en juillet, sera un congrès virtuel, le RSNA est, lui, d'ores et déjà annulé.

Si les JFR se tiennent effectivement en présentiel, la FNMR y sera bien évidemment et ce sera l'occasion d'une rencontre entre les membres de la famille radiologique libérale sur son stand.

SOMMAIRE – JUILLET 2020 # 435

Directeur de la publication : Dr Jean-Philippe MASSON • Rédacteur en chef : Dr Paul-Marie BLAYAC
Secrétaire de rédaction : Wilfrid VINCENT • Édition, secrétariat, publicité rédaction, Petites annonces : EDIRADIO - S.A.S. au capital de 40 000 euros
Tél. : 01 53 59 34 01 • Télécopie : 01 45 51 83 15 • www.fnmr.org • E-mail : info@fnmr.org • 168 A, rue de Grenelle 75007 Paris
Président : Dr Jean-Philippe MASSON • Responsable de la publicité : Dr Eric CHAVIGNY
Maquette : Cécile MILHAU • Crédits photos : Istock.com
IMPRIMERIE DECOMBAT : 5 bis rue Gustave Eiffel 15000 AURILLAC • Dépôt légal 1er trimestre 2020 • ISSN 1631-1914

Dossier :
Cybersécurité et imagerie

SOMMAIRE

Séminaire FNMR
Cybersécurité et imagerie
Janvier 2020

L'informatique est un outil de développement et de productivité pour les cabinets médicaux. Mais ces dernières années, des attaques contre les systèmes informatiques d'entreprises ont montré la vulnérabilité de nos réseaux. Plus récemment, plusieurs attaques au *ransomware*, ont visé dans notre pays le secteur de la santé : le centre hospitalier de Rouen, les cliniques du groupe Ramsay et un cabinet de radiologie.

La FNMR a organisé un séminaire en janvier dernier pour faire le point sur les menaces informatiques extérieures et les moyens d'y faire face.

Jean-Philippe Masson, président de la Fédération, a introduit la séance en soulignant la forte dépendance des cabinets de radiologie à l'informatique. Une panne peut bloquer l'activité. Elle peut, dans ce cas, s'assimiler à une panne de courant. Après réparation de la panne, le système peut repartir rapidement. En revanche, une attaque virale est plus difficile à gérer, elle a des impacts à terme.

Les différentes interventions présentées à l'occasion de ce séminaire et reprises dans ce dossier ont permis de mieux cerner les dangers des attaques informatiques, de rappeler la législation et d'aborder les moyens d'améliorer la sécurité de nos systèmes.

Dr Alvian LESNIK, radiologue

Cyber attaque : retour d'expérience

Dr Alvian LESNIK, médecin radiologue

Chaque centre d'imagerie peut être l'objet d'une attaque informatique du type de celle dont a été la victime le cabinet d'Alvian Lesnik.

C'est pourquoi il a voulu la présenter afin que chacun, dûment averti, puisse prendre les dispositions nécessaires pour éviter ce genre de dommages.

Tout commence en juin 2019 à l'ouverture du cabinet : *Docteur, rien ne marche, il n'y a pas de PACS, pas de RIS*[1]*, que fait-on ?* Ce n'est pas la première fois. Les informaticiens sont appelés. Le cabinet, patients compris, attend la remise en route du système. Enfin, la nouvelle arrive, nous avons été piratés. Le tour d'horizon montre que pratiquement plus rien n'est disponible : pas de RIS, pas de téléphone externe ou interne, le planning patients est indisponible, pas de PACS, pas de dictée, plus de réseau. La facturation n'est pas possible.

Heureusement, le scanner et l'IRM fonctionnent mais il n'y a pas de worklist. Les services GE et Syngovia (Siemens), qui équipent le cabinet, fonctionnent, mais il n'y a pas d'accès via le réseau, seulement un accès direct grâce aux consoles dédiées. Les échographes fonctionnent aussi mais toujours sans worklist. Idem pour les tables de radiographie mais il est impossible de les transmettre via le réseau sur les écrans. Il est donc possible de faire des radios mais pas de les imprimer. Il faut interpréter sur les écrans d'acquisition.

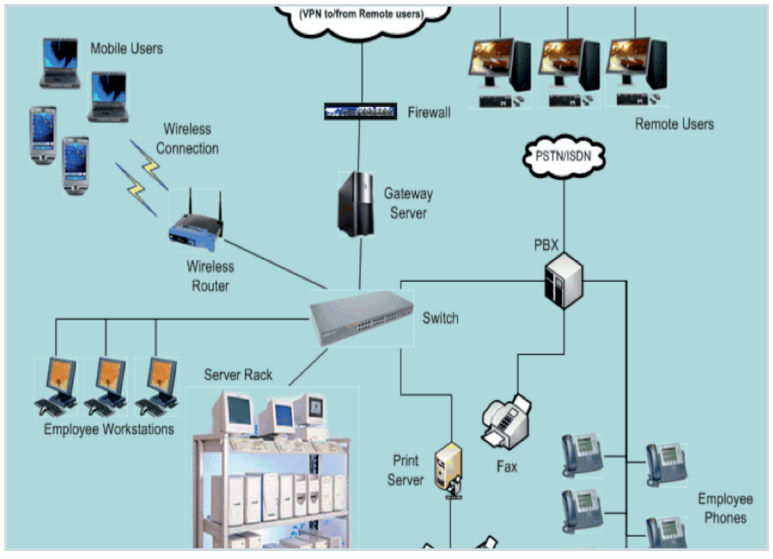
Les heures passent, et nous apprenons petit à petit qu'il y a un cryptage global des serveurs : serveurs de fonctionnement et serveurs de sauvegarde, sans pour autant que le virus ait franchi les barrières de sécurité de ces serveurs. Au total, 80 téraoctets de données ont été chiffrés.

Le virus, de type « beets » variante « Crysis » n'a pas de nom officiel. Il s'introduit dans les systèmes par le biais d'un partage de fichiers profitant d'une faille dans certains serveurs Microsoft sous système Samba. Il peut alors chiffrer l'ensemble des données du système. Il n'était pas répertorié dans l'antivirus utilisé par le cabinet à la demande du partenaire qui a installé notre RIS. En revanche, d'autres antivirus l'avaient repéré.

Quelques jours auparavant, le même type de virus avait touché la mairie de Baltimore aux États-Unis, en mai 2019.

On peut schématiser l'architecture informatique d'une structure radiologique en remplaçant dans le schéma ci-dessous certains ordinateurs par des scanners IRM échographes et des tables de radiologie. La connexion avec le « milieu extérieur » que constitue l'Internet est faite par le biais de passerelles sécurisées : les Firewall.

On obtient le schéma classique du « château fort » protégé par un mur d'enceinte, des postes de guet et un donjon central (serveurs et sauvegardes), lui-même protégé par des soldats et un poste de garde spécifique.



Un système informatique ouvert sur Internet

1. Picture Archiving and Communication System (système d'archivage et de transmission d'images), Radiological Information System (système d'information radiologique).

La caractéristique de l'attaque virale que nous avons subie est que le virus peut se déposer dans un poste périphérique connecté au réseau (par exemple mail sur un ordinateur) et pouvoir infecter l'ensemble des serveurs sans se soucier des Firewall de chacun des systèmes. C'est la fameuse « faille de sécurité » des serveurs sous système Microsoft Samba.
Le cryptage se fait en quelque sorte de l'extérieur.

Le résultat a été la paralysie de tout le système

Il a fallu revenir à Word, acheter en urgence des imprimantes branchées en direct sur un poste de secrétaire, un poste par service. Nous avons repris les cassettes audio, utilisé la dictée vocale de l'Iphone qui peut être transmise par SMS aux secrétaires. Il faut aussi revenir à la facturation papier.

Une fois le problème cerné, nous avons porté plainte à la gendarmerie. Il a fallu environ 48 heures pour que l'information remonte dans la haute hiérarchie. À partir de ce moment, nous avons reçu des appels que l'on peut retranscrire :

- *L'interlocuteur : Bonjour, je voudrais parler à l'informaticien.*
- *Le cabinet : Oui, à qui ai-je à faire ?*
- *L'interlocuteur : Je ne suis pas autorisé à vous donner mon nom.*
- *Le cabinet : Mais vous téléphonez d'où ?*
- *L'interlocuteur : Je ne suis pas autorisé à vous le dire.*

Ce qui motive ces autorités, c'est de récupérer les signatures virales en précisant : « *ne vous inquiétez pas, on a l'habitude, on va résoudre vos problèmes dans 24 ou 48 h* ». Et au bout de 24/48 h bien sûr : « *on n'a pas réussi à cracker le virus* », donc, débrouillez-vous.

Six mois avant l'attaque, nous avions eu une réunion avec tout les partenaires informatiques pour se mettre en conformité avec le RGPD. Nous avions mis en place des mesures avec un plan de reprise d'activité, des sauvegardes journalières sur NAS et la prise d'une assurance.

Comment en sommes-nous sortis ?

Nous avons rebâti tout le réseau pierre par pierre. Nous sommes partis d'un serveur sain, récupéré de l'extérieur et sur lequel nous avons branché, un à un, tous les systèmes. Il a fallu dé-viruser tous les ordinateurs, toutes les modalités d'imagerie une par une, et ça demande du temps. Nous avons soixante-huit imprimantes, cent cinquante ordinateurs, douze échographes, trois scanners, deux IRM, des ostéodensitomètres, des lecteurs de plaques, des capteurs plans, du matériel bureautique, des serveurs qui gèrent les imprimantes, un serveur qui gère le central d'appel téléphonique, etc.


© ENVATO

Nos prestataires sont multiples et variés, et nous n'avons pas le droit de toucher à leur matériel sous peine d'exclusion de garantie. Il faut donc appeler les prestataires un par un, pour qu'ils interviennent et passent tous les équipements aux antivirus. Certains sont réactifs, d'autres moins. Après analyse, il apparaît que nombre de matériels sont infectés donc inutilisables : le partage d'imprimantes, le serveur téléphonique, certains serveurs mais pas tous.

Dans le bilan du parc constitué avec des équipements d'âge très différents, nous constatons que certains ordinateurs anciens qui servent à des tâches « subalternes » comme le routage d'imprimantes ou la gestion des robots graveurs sont les plus dangereux.

Au final, nous ne disposons plus de planning alors que les rendez-vous étaient remplis à deux ou trois mois. Il est impossible de savoir quels patients viendront ou pas. Le serveur téléphonique est inutilisable pour les appels et les rendez-vous. Il faut maintenir la PDS[2] en doublant les astreintes manip et certains postes de secrétaires. Nous passons à la facturation papier. Nous ne pouvons plus accepter les cartes bancaires. Il faut garder une trace de tout ce qui se fait durant cette période de crise.

Les conséquences à moyen terme : une reprise progressive et lente de l'activité et faire le bilan des dommages pour l'assurance.

Pour remettre un embryon de système qui fonctionne, il faut six à dix jours.

Pendant cette période, il n'y a pas d'accès au PACS ni au RIS. Il n'y a pas de dictée vocale possible et les empreintes vocales sont perdues.

Le travail de secrétariat a été considérable pendant cette période comprenant aussi la récupération des informations pour chaque patient. En effet, toutes les sauvegardes ont été aussi cryptées. Nous avons seulement trouvé un ordinateur non crypté, ce qui nous a permis de récupé-

2. Permanence des soins

rer des données RIS et comptabilité avec une antériorité d'une quinzaine de jours. Si la base des comptes rendus a été à peu près récupérée, la base PACS des quinze jours précédents l'attaque a été perdue.

Une des leçons que nous tirons de cette expérience est qu'il faut que les télétransmissions soient à jour. Durant le black-out des quinze jours qui précède l'attaque informatique, nous n'avons aucune corrélation entre les fonds perçus et les écritures comptables.
La perte pour les forfaits techniques a été minime dans la mesure où nous étions en forfaits réduits. En revanche, la perte d'exploitation a été importante sur les honoraires, principalement pour les deux ou trois semaines qui ont suivi l'attaque virale avec une baisse significative de l'activité. Le bilan de fin d'année nous dira précisément quelles ont été les pertes. Il faut aussi tenir compte des frais complémentaires générés par cette attaque : les heures supplémentaires secrétaires, le doublement des manipulateurs d'astreinte, l'embauche de CDD, les heures supplémentaires des informaticiens, les prestataires externes en informatique dont certains ont travaillé 24/24.
Nos serveurs actuels sont sous séquestre dans le cadre de la procédure judiciaire en cours. Il a donc fallu acheter de nouveaux serveurs et d'autres matériels informatiques.
Même si ce n'est pas quantifiable, il faut tenir compte du stress, du sentiment de tourner en rond en participant à de multiples réunions.
Il a fallu également communiquer. L'information circule très vite, le patient arrive, on n'a pas donné de rendez-vous, on ne peut pas faire d'examen, pourquoi, comment, attaque virale, machin, donc allô, réseaux sociaux, etc. 48 h après l'attaque un premier article, non sollicité, était publié, les messages Facebook ou autres ont circulé. Nous avons publié un communiqué de presse. Mais que dire ? Nous avons joué la transparence : *oui, c'est un crypto virus avec une demande de rançon.*
À ce propos, quelle est la conduite à tenir. Nous avons eu un débat interne et voté pour la négociation. Mais nous nous rendons compte que la négociation prend du temps, qu'il ne faut pas être pressé pour faire baisser les prix. Nous avons négocié serveur par serveur. Nous avons finalement payé, pour voir, sur un serveur. Il faut bien comprendre que lorsque vous décidez de payer pour récupérer des données, le décryptage prend énormément de temps, 4 à 5 jours. Les données récupérées sont fragmentées. Qu'en faire ? Les réinjecter dans le réseau ? Sont-elles fiables ?

La conclusion, en fonction des nouveaux types de virus qui circulent, est qu'il faut disposer de sauvegardes hors réseau. Concrètement, lorsqu'une sauvegarde est faite, il faut couper physiquement le support du réseau. C'est relativement facile à faire avec peu de données comme pour les comptes rendus et les RIS. C'est beaucoup plus compliqué pour un PACS qui a un important volume de données.

> « Il faut également communiquer. L'information circule très vite »

Par la suite, notre assureur a mandaté une société pour auditer notre système. Son rapport comprend une trentaine de recommandations. Un réseau informatique doit être homogène alors que dans les cabinets ou les centres de radiologie ce sont des agrégats avec dix, quinze, parfois vingt prestataires, avec des matériels d'âges très différents, avec des versions Windows différentes. Il faut séparer physiquement le réseau intranet de l'extérieur. Les mises à jour de sécurité doivent être permanentes pour les antivirus et Windows. Certains équipements fonctionnaient avec Windows 7. Or, cette version du système d'exploitation ne bénéficie plus, depuis janvier, des mises à jour de sécurité gratuites.
Nos prestataires externes interviennent régulièrement pour faire de la maintenance avec une clé USB qu'ils vont brancher sur le réseau. Ces clés doivent être contrôlées systématiquement. Il ne faut pas non plus connecter les ordinateurs portables sur le réseau.

En dépit de toutes ces précautions, le risque d'être victime d'un hacker existe encore. Il faut donc s'organiser pour pouvoir rétablir son système le plus rapidement possible. C'est la question des sauvegardes protégées. Il faut savoir mettre en lieu sûr la comptabilité, les dossiers patients. La

© ENVATOELEMENTS

question est plus complexe pour les PACS. Les solutions cloud coûtent très cher en fonction du volume de données. Il n'y a pas de solution miracle.

Avec cette attaque, nous prenons conscience de notre grande dépendance à l'informatique. Les investissements iront croissant, informaticiens, matériels, sauvegardes. Parmi les recommandations, homogénéiser un parc trop hétérogène : Windows 7, Windows 10, Unix, Windows XP dans certains cas. Les scanners et les IRM, régulièrement renouvelés sont relativement faciles à mettre à jour. En revanche, quelle est l'informatique des tables de radiologie qui ne sont pas changées tous les cinq ans ? La même question se pose pour les graveurs de CD, les lecteurs de plaques, les routeurs, tout le petit matériel bureautique. Nos deux ostéodensitomètres présentaient des problèmes de sécurité dont un autre crypto virus pour l'un deux. Nous ne savons toujours pas depuis quand il avait infiltré l'équipement. Pire, un des ordinateurs de partage de réseau, oublié, était utilisé pour crypter … de la monnaie. Certains prestataires, vendeurs de matériels et de tables télécommandées, facturent les mises à jour Windows qui sont pourtant fournies gratuitement par Microsoft. Les raisons sont diverses : leurs matériels ne sont pas compatibles Windows 10, ils doivent installer de nouveaux logiciels hards ou softs, etc.

Il faut aussi aborder la question des assurances. Pour notre cabinet, l'assurance a permis de réduire les dommages même si elle ne rembourse pas tout. Il est clair que pour les nouveaux contrats, les assureurs vont demander des prérequis en matière de sécurité informatique.
Nous devons être aussi vigilants avec les personnes qui vont sur Internet ou répondent à des mails sur le réseau. Un audit est impératif. L'audit interne est insuffisant. Il faut passer par un audit externe. L'audit auquel nous avons procédé a révélé que les procédures d'un grand provider que nous utilisions n'était pas à jour.

Alors, lutte permanente entre attaque et défense, « Entreprises de santé », il faut ouvrir la presse et vous vous rendez compte que notre secteur est le nouvel eldorado des hackers, parce que nous sommes relativement peu protégés.

Me Joseph MÉOT, cabinet Choley et Vidal

Le règlement européen sur la protection des données et le délégué à la protection des données


DR

Maître Joseph MÉOT

Qu'apporte le RGPD ?

Fondamentalement, le RGPD (règlement général sur la protection des données) n'apporte pas grand-chose de nouveau en matière de réglementation. Ce qui change, c'est d'une part, la réglementation relative à la protection des données qui est harmonisée au niveau européen, et d'autre part, l'introduction de véritables sanctions. C'est donc un dispositif beaucoup plus répressif que celui que nous connaissions jusque-là.
Depuis le 25 mai 2018, tout le monde est censé être en conformité avec le RGPD. Je vous rassure, si vous ne l'êtes pas encore complètement, c'est aussi le cas de la plupart des intervenants et de la quasi-totalité des entreprises qui traitent des données, en particulier les petites et moyennes entreprises.

Pourquoi le RGPD concerne-t-il particulièrement les radiologues ? Parce que ceux-ci traitent de nombreuses données de nature médicale qui sont classées comme sensibles et qui font l'objet d'une protection spécifique.
La finalité du RGPD est de protéger davantage le citoyen face aux risques d'abus dans l'utilisation de ces données avec des sanctions qui peuvent être très lourdes. La CNIL[1], qui est l'autorité administrative chargée de veiller au respect de ce règlement, peut infliger des amendes pouvant

1. Commission nationale de l'informatique et des libertés

aller de 2 millions à 4 millions d'euros, soit 2% ou 4% du chiffre d'affaires. Cependant, la CNIL est avant tout dans une démarche d'accompagnement. Avant de prononcer des sanctions aussi sévères, il y a une série de mises en demeure, de recommandations qui sont émises. Les sanctions existent, il faut les prendre en compte, mais ne pas trop s'inquiéter. Elles n'arriveront pas d'un seul coup sans notification préalable.
Concernant les patients, leurs droits ne sont pas forcément nouveaux à l'exception du droit à la portabilité des données qui fait qu'un patient peut exiger de vous la communication de ses données personnelles à un autre professionnel de santé.
Hormis ce droit d'accès, il y a aussi le droit de rectification et le droit à l'oubli.

Pour le droit à l'oubli, revenons sur ce patient qui vous demande effectivement de supprimer des données de son dossier médical pour une raison X ou Y. Cette demande entre en conflit avec votre obligation de conserver les données médicales pour pouvoir vous couvrir en cas de contentieux. Dans ces cas-là, je vous conseille de privilégier votre couverture par rapport à la demande du patient, les risques pour vous sont quand même plus importants si le patient engage un contentieux et que vous n'avez aucun moyen de vous défendre, parce que vous avez supprimé à sa demande les dossiers médicaux. **S'agissant du délai de conservation des données médicales,** la prescription est de dix ans pour les mineurs. C'est-à-dire dix ans à partir de l'âge de la majorité. Mais en pratique, je vous conseille de les conserver non pas dix ans mais trente ans. En effet, des problèmes peuvent surgir beaucoup plus loin que le délai de dix ans. Par exemple, dans le cas d'un contentieux du patient au niveau de son état physique alors que la date de consolidation est assez éloignée de l'examen en litige. Il faut donc calculer dix ans à partir de la consolidation. À partir de cette date, le patient dispose de dix ans pour agir.
Le RGPD, sans créer réellement de nouveauté au niveau de la responsabilité, renforce celle de la personne en charge du traitement des données. En l'occurrence, vous, s'agissant des données de vos patients et également celles de vos sous-traitants auxquels vous pouvez recourir. Toutefois, il faut préciser que le recours à des sous-traitants n'entraîne pas une décharge de responsabilité et vous avez tout de même l'obligation, ne serait-ce que de vérifier que ce sous-traitant présente des garanties suffisantes pour s'assurer du respect du RGPD.

Concernant la mise en conformité des données personnelles que vous détenez sur vos patients, éventuellement sur votre personnel, ce qui est important, c'est, d'abord, d'en établir une cartographie. Cela consiste repérer où sont les données, qui y a accès, comment elles circulent, quels sont leurs flux de circulation et quelles sont leurs finalités. En fonction de cette cartographie, vous pourrez vous mettre en conformité avec la réglementation RGPD en organisant un traitement des données en fonction de leur finalité et en restreignant l'accès en fonction des besoins.

Pour protéger les données, le RGPD impose la mise en place d'un système de sécurités spécifiques. Elles visent à permettre la conservation des données mais aussi qu'elles ne soient pas diffusées sans le consentement des personnes concernées. Il faut insister sur le risque d'accès non autorisé aux données, y compris le risque de piratage. Mais il faut aussi assurer l'intégrité des données. En cas de méconnaissance de ces obligations en matière de sécurité et en l'absence de fixation de garde-fous sécuritaires, vous risquez des sanctions de la part de la CNIL qui, encore une fois, seront précédées d'accompagnement, ce qui vous permet de vous mettre en conformité.

Il est essentiel de vérifier que les sous-traitants auxquels vous faites appel sont, eux aussi, en conformité avec le RGPD, ou en tout cas présentent des garanties suffisantes et en particulier pour le stockage des données en externe. Il faut choisir un hébergeur qui exerce dans le cadre du territoire du RGPD et donc qui les héberge en Europe plutôt qu'à l'extérieur – aux États-Unis ou comme cela se développe en Asie – où vous n'aurez aucune garantie de sécurité et de respect des droits des utilisateurs.

Le Data Protection Officer

Le RGPD a introduit un nouvel acteur, le Data Protection Officer (DPO), le délégué à la protection des données (DPO) en français. Il succède à l'ancien correspondant informatique et liberté de la législation française.
Les différences entre cette précédente et cette nouvelle entité sont des prérogatives considérablement renforcées et le DPO obligatoire dans un certain nombre de cas.

Quelle est sa mission ?

Le DPO est chargé de veiller de manière indépendante à la conformité en matière de protection des données. Indépendant, cela signifie que le DPO ne doit pas exercer de fonctions décisionnelles au sein de l'organisme qui a recourt à ses services. Il ne doit pas non plus être subordonné à l'organisme par lequel il a été désigné.
Le DPO est avant tout un coordinateur. Il a une mission d'information, de conseil et d'audit auprès de l'entité qui l'a désigné. Il est également l'interlocuteur auprès de l'organisme qui est chargé de

veiller au respect de la réglementation en matière de données personnelles, à savoir, en France, la CNIL. Quelles sont exactement les missions du DPO auprès de l'organisme ? La première est d'informer et conseiller le responsable du traitement ou le sous-traitant, ainsi que les employés. Cela permet de les tenir informés sur les normes du RGPD, de les conseiller sur les règles à suivre en matière de sécurité, sécurité informatique notamment. La seconde est un contrôle du respect du règlement national –mais aussi de la réglementation européenne– en matière de protection des données.
Il conseille l'organisme pour prendre les moyens nécessaires pour assurer la mise en conformité et notamment, il conseille l'organisme dans le cadre de la réalisation des études d'impact sur la protection des données et en vérifie l'exécution. En effet, lorsque vous faites votre mise en conformité au RGPD, il faut faire des études d'impact sur votre activité et sur cette protection des données. Le DPO est là pour vous conseiller dans le cadre de ces démarches. Enfin, il est l'interlocuteur privilégié entre vous et la CNIL.

Le DPO doit remplir trois conditions. La première, est de disposer d'un statut qui lui confère la capacité d'agir en toute indépendance. Il ne doit recevoir aucune instruction, ni pouvoir faire l'objet de sanctions de la part de l'organisme qui l'emploie, en tout cas dans le cadre de sa mission. Il bénéficie d'une certaine protection. D'autre part, il ne peut pas engager. Ce n'est pas lui qui prend les décisions en matière de traitement des données, sinon il y a conflit d'intérêts entre sa fonction et celle de gestionnaire des données.

La deuxième condition porte sur ses compétences. Le DPO doit réunir trois compétences. Il doit bien connaître la réglementation en matière de protection des données. Il doit être compétent en matière de traitement de ces données, en pratique c'est surtout une connaissance en matière informatique. Précisons que le RGPD concerne les données personnelles informatiques, mais pas seulement, par exemple les dossiers papier de patients sont également soumis au règlement. Enfin, le délégué doit avoir une compétence dans le domaine de l'entité pour laquelle il intervient. Donc, concernant un cabinet de radiologie, il doit savoir comment il fonctionne, quelles sont les nécessités en matière médicale et pourquoi vous traitez des données, quelles sont les finalités des traitements que vous mettez en œuvre.

Enfin, le DPO doit disposer de moyens suffisants, ce qui implique qu'il soit disponible et joignable. Il n'intervient pas seulement au moment de votre première mise en conformité au RGPD. Il ne peut pas se dire, j'ai fini ma mission, l'entreprise est conforme, je n'ai plus à intervenir. En fait, le DPO est un acteur qui est là pour intervenir tous les jours avec vous et faire en sorte que vous mainteniez votre conformité au RGPD dans le temps. Pour cela, il faut qu'il soit disponible et en capacité, qu'il ait du temps pour intervenir dans votre organisme. Si par exemple vous avez désigné comme DPO un de vos employés, un manipulateur par exemple, celui-ci doit avoir le temps suffisant pour exercer sa mission de DPO. Ce n'est pas juste un poste que l'on nomme pour être conforme à la réglementation. Il doit également disposer des moyens matériels et humains adéquats pour pouvoir intervenir. Il doit être associé à vos projets. Il faut le tenir informé des projets que vous mettez en place dans le cadre du traitement des données personnelles. Ainsi, si vous recevez un nouvel appareil, il faut tenir votre délégué informé pour qu'il puisse voir comment le nouvel équipement va traiter des données personnelles et comment il va le placer à l'intérieur de l'architecture pour faire en sorte que sa gestion et celle des données qu'il contient soient conformes à la réglementation.

Le DPO est-il obligatoire ?

Oui, pour les autorités ou organismes publics, les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle. Il est également obligatoire pour les organismes dont les activités de base les amènent à traiter à grande échelle des données dites sensibles ou relatives à des condamnations pénales et infractions.
Les radiologues sont concernés par le troisième point sur le traitement des données dites sensibles dont les données médicales.

Le RGPD précise que pour que le DPO soit obligatoire, il faut que les données sensibles soient traitées à grande échelle. Les organismes contrôleurs européens se sont réunis pour essayer d'expliquer quel était le seuil à partir duquel nous pouvons considérer qu'il s'agit de traitement à grande échelle. Ils ont donné une série d'exemples et notamment le traitement de dossiers patients par un hôpital qui est donc obligé d'avoir un DPO. En revanche, le traitement des données de patients par un médecin libéral, même si ce sont des données sensibles, n'est pas suffisamment important en volume pour que le DPO soit obligatoire.
Il est vrai que pour certains cabinets libéraux, par exemple en matière de radiothérapie, il y a beaucoup d'associés, beaucoup de patients et des traitements de données qui sont d'une certaine importance. Il est donc possible d'être

à la limite entre le seuil à partir duquel c'est obligatoire et en dessous duquel ça ne l'est pas. Mais, même si le DPO n'est pas obligatoire, c'est un moyen assez efficace pour le radiologue de pouvoir se mettre en conformité avec le RGPD. Nous recommandons donc assez fortement le recours à cet intervenant. Du fait que vous traitez des données sensibles, les autorités de réglementation vont toujours être plus rigoureuses avec vous.

Pour ces raisons, il est important pour les médecins, et en particulier les médecins radiologues, d'être au maximum en conformité avec le RGPD, de se doter de l'ensemble des moyens nécessaires pour permettre cette mise en conformité. Une expertise juridique, et pas seulement technique, doit vérifier la conformité au RGPD.

Le DPO n'est pas juste un informaticien qui vient vérifier que vos systèmes de sécurité sont bien réglés. Il doit proposer des plans d'action, des architectures pour que votre système soit sécurisé. Il le fait au regard de critères qui sont imposés par la réglementation. Et pour cela, il faut qu'il connaisse véritablement cette réglementation, donc ce n'est pas juste un technicien.

Quels sont les critères de choix d'un DPO pour un radiologue ?

Le RGPD explique clairement comment une entité, un radiologue par exemple, doit choisir son DPO. Il doit être désigné sur la base de ses qualités professionnelles et en particulier de ses connaissances spécialisées du droit, donc la connaissance de la réglementation en matière de données personnelles et des pratiques en matière de protection des données. Il faut aussi tenir compte de son expertise technique, notamment en matière informatique, de sa capacité concrète à accomplir ses missions, soit de sa disponibilité et de ses moyens matériels et humains.

Le RGPD précise aussi que le DPO doit donner ses conseils sur les opérations de traitement des données compte tenu de la nature de la portée du contexte et des finalités du traitement. Cela signifie qu'il doit connaître le domaine dans lequel vous exercez et les finalités du traitement de vos données : pourquoi vous traitez les données, pourquoi vous avez besoin de traiter des données et leurs natures.

Il est possible de recourir à un prestataire externe comme DPO ou à un agent interne à l'organisation qui le désigne. Il est donc possible de choisir un membre du personnel du cabinet dans lequel vous exercez. Mais attention, il est compliqué de choisir un employé sur lequel le radiologue a des pouvoirs de direction et de sanction et en même temps de respecter son indépendance. Ça remet en cause le principe même du délégué.
C'est pourquoi, en particulier dans une structure de taille moyenne ou petite, nous conseillons de recourir à un prestataire externe, sachant qu'il est possible pour plusieurs radiologues et plusieurs cabinets de radiologie de désigner un DPO commun à l'ensemble des cabinets et éventuellement de mutualiser le coût de son intervention.

La présence d'un DPO n'exonère pas le radiologue de sa responsabilité dans le traitement des données. Ce n'est pas le DPO qui garantit la conformité du cabinet au regard du RGPD. Ce n'est pas lui, non plus, qui sera sanctionné en cas de manquements. Le DPO est un conseiller, un coordinateur et un lanceur d'alerte. Il pointe d'éventuels problèmes, propose des solutions pour la mise en conformité. Le DPO a donc une obligation de moyen, pas de résultat. Vous pourrez vous retourner contre lui si vous estimez qu'il a manqué à ses obligations d'information et de conseil mais le radiologue conserve la responsabilité au regard de la CNIL.

Gilles CASTÉRAN, directeur exécutif Accenture Security

Cybersécurité et cyber-résilience

En matière de cybersécurité, les événements qui se produisent au niveau mondial, dans les grandes organisations, sont exactement les mêmes que ceux que vous vivez localement dans vos entreprises.

Je vais vous parler de cybersécurité mais aussi de cyber-résilience, c'est-à-dire que faire pour rester opérationnel, continuer à travailler alors que nous venons de subir une cyberattaque. Comme le Dr Lesnik l'a décrit au travers de l'expérience de son groupe.

Un autre point important a été abordé lors de ce séminaire, c'est l'architecture des systèmes d'information, le rôle de l'architecte indépendant. L'architecture, ce n'est pas seulement concevoir un système d'information en partant de zéro, c'est aussi concevoir la transformation pour le faire évoluer de façon cohérente.

Gilles CASTÉRAN

Ce qui a été évoqué jusqu'à présent susciterait plutôt de la défiance à l'égard du numérique, or, nous recherchons à construire une relation de confiance avec les patients.

Nous vivons dans un monde qualifié sous l'acronyme VICA (Volatilité, incertitude, complexité, ambiguïté). Ce concept a été défini par l'armée américaine dans les années 1990. Cela signifie que la révolution digitale rend notre monde extrêmement volatil. Les changements ont une amplitude qui n'a jamais été aussi rapide. Le monde est devenu incertain au sens où nous ne pouvons plus prédire. Par exemple, personne n'aurait pu envisager le Brexit même si après coup, il nous semble « évident » que nous aurions pu le prévoir.
Nous vivons dans un monde de plus en plus complexe qu'il faut distinguer de « compliqué ». Construire un avion c'est compliqué, mais nous savons faire. Il faut de l'intelligence, des procédures ont été établies. Soigner des patients, c'est complexe parce qu'il y a des relations, des interactions humaines. Notre monde est aussi ambigu. Tout événement nouveau est ambigu. Il a deux lectures. C'est le cas des systèmes d'information dont nous venons de voir les risques mais qui ont également changé nos métiers, changé nos vies, permis de diffuser de l'information, de la culture, favoriser l'éducation du plus grand nombre, et sauver des vies.

Nous vivons dans un monde VICA, ce qui implique que **tous les concepts de cybersécurité ou de résilience qui avaient été définis il y a quelques années ont volé en éclats** et ne fonctionnent plus. Concrètement, par le passé, la cybersécurité, c'était une architecture en mode château fort. Un réseau était protégé de l'extérieur. Mais nous découvrons maintenant qu'il peut être attaqué de l'intérieur. Certains de ses composants, intérieurs, peuvent être extrêmement vulnérables. Nous devons repenser les architectures.
Une autre vulnérabilité provient de l'interdépendance entre tous les composants, les partenaires, les personnes avec qui vous travaillez, vos patients.

La santé est un des domaines d'activité très compliqué pour plusieurs raisons. D'une part parce qu'il y a d'ambitieux projets digitaux. Il y a tous les jours de nouvelles initiatives autour de la santé que ce soit pour le parcours du soin, avec le health data hub pour le partage de données. La multitude de données qui apparaissent – avec l'arrivée de tous les nouveaux services comme la télémédecine, les services aux patients avec l'espace patient– crée évidemment des nouvelles menaces.
Mais c'est aussi une très bonne nouvelle. C'est la conséquence de nouveaux usages du numérique, d'une nouvelle dynamique, il faut d'abord le regarder sous cet angle-là. En effet, toute transformation, toute évolution implique des risques.

Avec le plan « Ma Santé 2022 », **les initiatives digitales dans le domaine de la santé se multiplient et se pose**

donc la question des données. Le nombre et la diversité des acteurs de ce secteur compliquent encore le problème – établissements, professionnels, cabinets médicaux. Cette organisation rend plus difficile la protection collective contre des menaces qui sont de plus en plus sophistiquées. Les attaques évoluent et sont de plus en plus difficiles à détecter et à identifier. Il faut du temps pour comprendre exactement la nature et l'ampleur de l'attaque. De leur côté, les organismes d'État en charge de la cybersécurité cherchent à comprendre la nature des attaques, les conditions de propagation mais ils ne sont pas toujours présents pour aider les victimes.

Nous sommes entrés dans le monde digital, il faut le gérer. Le risque est de plus en plus impactant et votre secteur est un des plus ciblé. Est-il plus fragile ? A-t-il une appétence à payer plus facilement ? … En tout cas, c'est un secteur très ciblé, comme en général les professions libérales. Ce qui complique encore la situation est que vous avez des dispositifs médicaux dont les cycles de vie sont en inadéquation avec le cycle de vie du digital. C'est la fragilité la plus importante de votre secteur. C'était vrai dans les télécoms il y a une dizaine d'années, et aujourd'hui dans l'industrie qui multiplie les équipements industriels de plus en plus connectés, qui intègrent de plus en plus de technologies, de systèmes d'information.

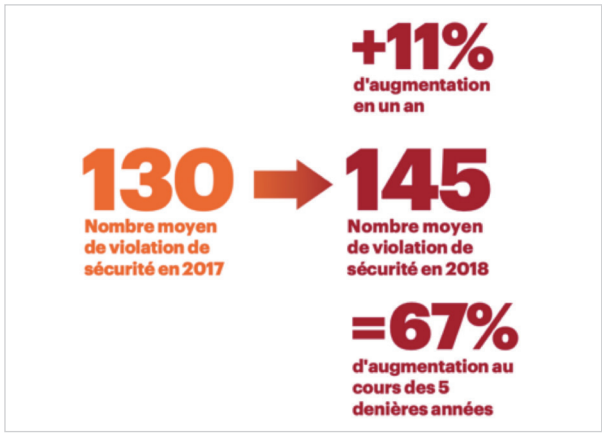
C'est une vraie difficulté que de gérer le cycle de vie de l'ensemble des composants de vos équipements, de vos dispositifs, ce qui fait que vous êtes très exposés aux attaques.

Il y a différents types d'attaquants. Dans le cas exposé par le Dr Lesnik, il s'agit plutôt d'escroquerie. Mais il y a aussi des hacktivistes, qui ciblent des entreprises d'un secteur, comme le secteur pétrolier par exemple. Il faut aussi tenir compte du risque de négligences ou d'actes malveillants de la part des employés. Les concurrents peuvent constituer une menace. Enfin, des États Nation financent de la R&D pour concevoir des attaques digitales. Ainsi, des entreprises ont été victimes, il y a deux ans, du ramsonware. NotPetya, qui pourrait être développé pour cibler les organisations ukrainiennes lors du conflit entre la Russie et l'Ukraine.

Chez Accenture, nous faisons des études très précises sur l'économie de la cybersécurité. Au niveau mondial, sur un panel de plus de 4000 entreprises issues de onze pays, nous observons une forte augmentation des menaces, de 11% en 2018. Sur cinq ans, la progression du nombre de violation par entreprise est de 67%. Les intrusions dans les systèmes des entreprises deviennent donc une réalité commune.

Le coût de la cybersécurité est également en forte progression. Il comprend ce qui est nécessaire pour se protéger, pour détecter, pour remédier, pour réparer mais aussi tous les impacts comme la perte de valeur, l'impact de l'image, le coût de l'assurance. La croissance des coûts de la sécurité est de 17% sur 2018 et de 72% sur les cinq dernières années. Mais, heureusement, l'efficacité des équipes qui protègent les entreprises augmente en passant de 70% de succès dans la défense d'attaques ciblées à 87% de 2017 à 2018.

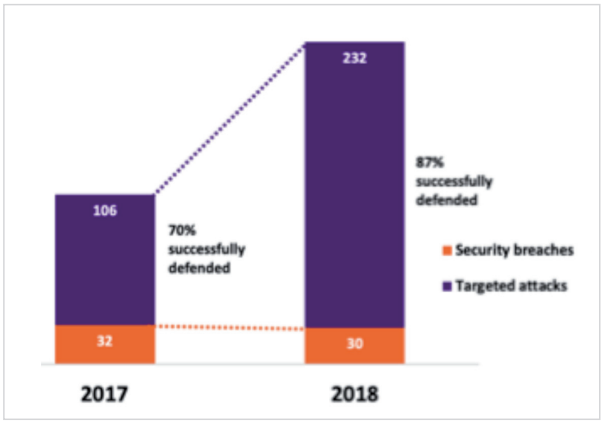
En 2019, 40% des attaques que subit une entreprise sont issues de son écosystème. Ce qui a complètement changé, c'est que même les entreprises qui se protégeaient bien de l'intérieur, qui mettaient toutes les bonnes pratiques pour se protéger se font attaquer à travers leur écosystème, c'est-à-dire leurs sous-traitants, partenaire. Ce n'est évidemment pas le sous-traitant qui attaque mais il est une porte d'entrée pour l'attaquant.



C'est ce qui s'est produit, en France, avec l'attaque de grandes l'entreprises spécialisées dans le service informatique, afin d'atteindre des grands groupes. Cette entreprise travaille pour Airbus et les constructeurs automobiles. Elle a été attaquée mais c'est Airbus qui était ciblé.

Le paradigme de la cybersécurité change. Maintenant, **il ne faut pas seulement se protéger soi-même, mais il faut protéger l'ensemble de son écosystème** ou garantir que l'ensemble de l'écosystème a la même maturité de protection, sinon des vulnérabilités assez fortes se créent.

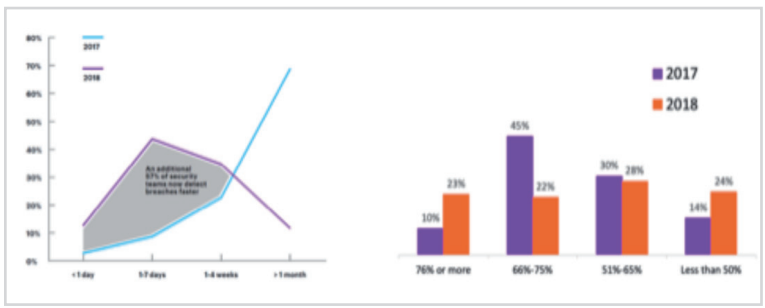
Les analyses nous montrent aussi que la détection des violations est de plus en plus rapide. En 2017, quelques pourcents étaient détectés en une journée, il y en a 10% en 2018 sur un volume important. En revanche, on constate qu'en 2017, 10% des entreprises détectaient 76% des intrusions et 23% en 2018. Mais 14% des entreprises détectaient moins de 50% des intrusions en 2017 et 24% en 2018. Ces chiffres démontrent que les entreprises les plus matures se sont améliorées alors que les « moins matures » ont réduit leur capacité de détection. C'est logique puisque les attaques sont de plus en plus



sophistiquées, impactantes et ciblées.
Une des grandes transformations digitales réside dans l'arrivée de nouvelles technologies, comme le cloud ou des clouds hybrides, qui simplifie grandement la gestion du système d'information. Dans les clouds hybrides, une partie de votre système d'information est dans le cloud et l'autre peut être hébergée chez vous.
D'autres évolutions, comme l'intelligence artificielle ou la blockchain créent de nouvelles vulnérabilités tout en permettant également de contribuer à sécuriser une grande partie des données avec des mécanismes complètement délocalisés.

Que font les leaders pour assurer la cybersécurité ?

C'est assez basique, ils appliquent les fondamentaux de la cybersécurité à l'échelle de toute l'entreprise et de son écosystème. L'écosystème d'une grande entreprise, c'est toute sa chaîne de valeur. Ça comprend ses filiales, ses partenaires, ses fournisseurs…



Un autre point clé est la formation. Les entreprises les plus matures en cybersécurité investissent plus en formation des équipes. Rappelons qu'une grande partie des menaces sont internes. Il est donc essentiel de sensibiliser aux attaques sur le fishing, par exemple. Il faut s'entraîner, faire des tests à grande échelle. Il faut passer d'une culture de la conformité à une culture de la sécurité. Cela consiste à appliquer les bonnes règles pour se protéger individuellement et collectivement.

Le troisième point est la collaboration. Ceux qui réussissent le mieux sont ceux qui partagent le plus, en particulier au sein d'un même secteur d'activité. Comme les attaques sont de plus en plus ciblées, il est très vertueux de partager les retours d'expériences. Il faut aussi collaborer avec les partenaires, les accompagner pour qu'ils soient à niveau. Il faut être intransigeant sur les règles de mise à jour des composants sur chacun de vos équipements. Normalement, il y a des homologations qui sont faites pour ça. Il faut être rigoureux avec les fournisseurs d'équipement et les évaluer.

Pour résumer, la cybersécurité nécessite de mettre en place une gouvernance favorisant la maîtrise des risques, déployer les fondamentaux en s'entraîner, et se focaliser sur la protection des données. Il faut avoir une vision architecturale qui suppose de comprendre : où sont les données et avec qui elles sont partagées, quel est le cycle de vie des données.
Il faut aussi déterminer ce qui est essentiel pour l'activité ce qui suppose une architecture du système d'information résiliente en cas d'attaque en mettant en place des architectures adaptatives au regard du risque numérique et donc d'acquérir des compétences d'architecture et de risque management.
En terme d'hygiène de sécurité, il est essentiel d'appliquer les basiques : une politique de mots de passe, des mises à jour régulière des composants, faire des sauvegardes et les tester.

Et puis entraînez-vous à la gestion de crise.

OptiJECT®

loversol

La **solution d'injection** prête à l'emploi au scanner

KITS OPTIJECT®
AVEC NÉCESSAIRE D'ADMINISTRATION

- Utilisation simplifiée et sécurisée
- Concentrations et volumes adaptés à votre pratique quotidienne

Optiject® est indiqué en tomodensitométrie.
Conformément à la stratégie diagnostique recommandée par la HAS de décembre 2018 : Les produits tri-iodés hydrosolubles, très utilisés en scanner et en angiographie, ont remplacé les produits iodés ioniques. Les explorations radiologiques utilisant Optiject® se font selon le Guide du bon usage des examens d'imagerie médicale réactualisé en 2013 par la Société Française de Radiologie (http://gbu.radiologie.fr/), qui place dans la stratégie diagnostique, les examens suivants : tomodensitométrie du crâne, tomodensitométrie corps entier, urographie intraveineuse, phlébographie, coronarographie, ventriculographie, aortographie, artériographie rénale, artériographie périphérique, artériographie viscérale, artériographie cérébrale, angiographie numérisée.

Guerbet

COMMITTED*

* L'engagement Guerbet

Médicament soumis à prescription médicale. Remboursement et agrément aux collectivités.
OptiVantage® : est un système d'injection de produit de contraste à double tête fabriqué par Liebel-Flarsheim Company LLC. Dispositif médical de classe IIb, conforme à la directive 93/42/CEE, réservé à l'usage des professionnels de santé, non remboursable. Chaque opérateur qui utilise un injecteur **OptiVantage®** doit avoir suivi une formation à son utilisation. CE0123.

Guerbet France s'engage, au travers de sa politique qualité, au respect de la charte de l'information par démarchage ou prospection visant à la promotion des médicaments ainsi que son référentiel. Les délégués médicaux Guerbet France se tiennent à votre disposition pour répondre à toute question relative aux règles de déontologie de l'entreprise.

Pour une information complète, consultez le Résumé des Caractéristiques du Produit sur la base de données publique du médicament en flashant ce QR Code.
Ou directement sur le site internet :
http://base-donnees-publique.medicaments.gouv.fr

PF1972 – Juin 2020 – 19/10/62823503/PM/004 – Conception : ANNAPURNA 8000 – Photos : Shutterstock – Réalisation : cn communication

Dr Christian FORTEL, radiologue

Le RGPD, règlement général pour la protection des données

Le RGPD désigne le Règlement Général à la Protection des Données. C'est une loi qui est applicable depuis le 25 mai 2018.

Historiquement, c'est une décision européenne qui a des conséquences pour toutes les sociétés qui utilisent ou qui hébergent des données dans l'Union européenne. L'état d'esprit du RGPD est d'assurer une protection de ces données pour éviter en particulier l'utilisation commerciale, comme nous avons pu le voir, par de grandes sociétés internationales. Les données sont une source de richesse commerciale importante pour des entreprises comme les GAFA[1], par exemple.

Dr Christian FORTEL, médecin radiologue

Le RGPD s'impose depuis deux ans. Si au départ l'idée de ce qu'il impliquait était un peu floue, elle est plus précise aujourd'hui. Forcomed a conçu une formation qui permet de comprendre ce que ce nouveau règlement apporte aux entreprises de radiologie et comment le mettre en pratique au quotidien.

Une première lecture laisse à penser que le RGPD met en place une réglementation plus stricte que celle de la CNIL[2] en y ajoutant des sanctions qui peuvent aller jusqu'à 4% du chiffre d'affaires (CA) ou 4 millions d'euros pour des pénalités graves. Les pénalités plus légères peuvent représenter 2% du CA ou 2 millions d'euros.

Pour les cabinets, la mise en conformité avec le RGPD nécessite un travail important de mise en place et de suivi. Il faudra également s'assurer dans le temps, en cas de contrôle, du respect de la conformité. Ce qu'il faut retenir, c'est qu'il ne faut pas se précipiter pour éviter une sanction mais se mettre en conformité de façon à ce qu'en cas de contrôle le cabinet puisse se protéger, se prémunir des sanctions. Au début, en pratique, la CNIL pourra intervenir pour mettre en place des procédures d'alerte, éventuellement des mises en demeure. Elle pourra aussi assurer un accompagnement à titre de conseil pour les sociétés qui ont commencé à mettre en place les différentes procédures.

Délégué à la Protection des Données (DPO)

En premier lieu, il faut trouver un responsable. La question est différente selon que vous êtes un groupe important ou une petite structure, parce qu'il faut désigner ce que l'on appelle un délégué à la protection des données, le DPO. Pour les sociétés importantes, le plus simple semble être d'avoir recours à un prestataire externe qui puisse assurer cette fonction et cet accompagnement.

Pour les petites structures de radiologie, ce n'est pas une obligation au vu du volume des données utilisées. Si dans votre groupe, un radiologue a une compétence particulière, si vous avez un informaticien ou une secrétaire, un manipulateur qui aurait vraiment une compétence, il est possible de le désigner comme DPO.

Ce n'est pas une fonction à prendre à la légère. La tâche est lourde, chronophage, complexe. Le DPO doit mettre en place la procédure, former le personnel et assurer une information auprès des patients. S'il y a un contrôle de la

1. Google, Apple, Facebook, Amazon
2. Commission nationale de l'informatique et des libertés

CNIL, c'est lui qui doit assurer la présentation du registre tel qu'il le tient.
Pour une structure importante, la question est le choix du prestataire. Il semblerait que certains cabinets d'avocats puissent proposer cette prestation. En effet, il faut une double compétence juridique et informatique. Dans le cas du recours à une société informatique, il faut faire attention au risque de conflit d'intérêt si elle fournit le RIS ou le PACS. Il n'est, en effet, pas possible d'être fournisseur et contrôleur.
Dans notre cabinet comprenant une vingtaine d'associés, nous faisons le choix d'un prestataire externe faute de temps disponible et de compétences internes.

Délégué à la protection des données (DPO) Il n'est pas possible d'être founisseur et contrôleur

Information des patients

L'information des patients fait partie des obligations du RGPD. Comment la faire et quels sont les droits des patients ?
L'esprit de la loi veut que l'information communiquée au patient soit claire, compréhensible. On pourrait dire qu'elle doit être *telle que l'on pourrait s'adresser à un enfant et qu'il puisse la comprendre*. Cela signifie qu'il n'est pas possible de se contenter de déposer un cahier dans un coin de salle en considérant qu'il est accessible. L'information doit être réellement accessible, claire et assez concise.

Le plus simple pourrait être d'assurer un mode d'affichage à l'accueil ou dans les salles d'attente. Il est aussi possible de diffuser l'information par le site Internet du cabinet qui peut comprendre des informations complémentaires.
Chaque patient doit être informé que, grâce au RGPD, il a un droit d'accès à ses données. Il a également le droit de rectifier les données si, par exemple, il y a des erreurs ou si des données ont été conservées sur une durée trop longue ou encore si des données confidentielles sont conservées alors que le patient ne le souhaite pas.
Le patient peut aussi exercer un droit à la portabilité. C'est la possibilité de demander que les données conservées par un cabinet de radiologie soient mises à la disposition d'un autre cabinet.
Le patient doit aussi être informé qu'il peut saisir la CNIL sur une difficulté qu'il aurait rencontrée soit en matière d'accès aux données, soit sur une rectification qu'il n'aurait pas obtenue.

Le RGPD apporte donc des droits supplémentaires aux patients. Il introduit aussi une notion de transparence. Tout doit être écrit, traçable. Il faut dont rédiger des protocoles qui serviront à former le personnel pour qu'il puisse répondre aux demandes des patients.

Mettre en pratique le RGPD dans les cabinets

Il faut commencer par rédiger un registre. Le site de la CNIL en présente un exemple sous forme d'un tableau Excel. Le registre va servir à établir une cartographie exhaustive sur toutes les données que les radiologues ont à leur disposition. D'où viennent-elles ? Des patients. Elles comprennent leur nom, leur adresse, leur mode de vie, leurs antécédents. Tout ce dont on se sert en médecine : est-il diabétique ? A-t-il du cholestérol ? etc.
Les données concernant les personnels, les manipulateurs, les secrétaires mais aussi les comptables, le personnel administratif doivent être aussi cartographiées.

Vos fournisseurs – de RIS, de PACS – doivent aussi s'engager à vous fournir un document qui certifie qu'ils respectent le RGPD. En cas de contrôle, le cabinet de radiologie devra présenter ce document. Il y a un partage de responsabilité.

La cartographie est extrêmement importante, précise. Elle impose d'être vigilant. Vous utilisez vos ordinateurs, vos tablettes, vos téléphones, des clés USB, des disques externes sur lesquelles vous pouvez être amenés à mettre des documents, des dossiers de patients, etc., qui peuvent être plus facilement piratés. Tous ces supports peuvent être aussi contrôlés par la CNIL. Ils doivent faire partie de la cartographie.

Il faut aussi savoir différencier ce que l'on appelle les données de santé. Les radiologues sont particulièrement visés par le RGPD parce qu'en tant que profession de santé nous disposons d'éléments de données extrêmement sensibles. Le patient dispose du droit à l'oubli et dans le même temps, le radiologue est soumis au droit de conservation des données puisque sa responsabilité peut être appelée en cas de contrôle de la sécurité sociale ou de procédure juridique. Le délai légal de conservation est de dix ans.

Il y a donc d'un côté le droit à l'oubli et de l'autre une obligation de conservation. Le RGPD fait un cas particulier pour les professionnels de santé et pour les radiologues en particulier qui n'ont pas besoin de demander le consentement des patients pour conserver leurs antécédents médicaux, etc. Dans l'esprit du RGPD, les professionnels de santé peuvent conserver ces données dans la mesure où il s'agit de données de santé, c'est-à-dire celles qui sont utiles pour les diagnostics, pour les antécédents, etc. Il faut donc distinguer les données de santé et s'interroger sur l'intérêt médical d'autres données comme le mode de vie du patient, sa religion, ses habitudes sexuelles. Elles peuvent, dans certains cas, être indispensables médicalement comme pour les infections sexuellement transmissibles, dans d'autres cas non. Si les données n'ont pas d'intérêt médical, il faut obtenir le consentement du patient pour les conserver.

Le registre doit retracer de façon exhaustive toutes les mesures de sécurité techniques ou organisationnelles mises en place. Il faut préciser les délais d'effacement qui sont de dix ans pour les radiologues du point de vue médico-légal. Il faut aussi mentionner les flux de destinataires, donc mentionner les destinataires des données, quelles données sont envoyées, comment elles le sont, qui y a accès, les secrétaires, les manipulateurs. Le personnel administratif a-t-il accès aux données ? Si oui, aux quelles précisément et pas forcément les données médicales mais seulement d'ordre administratif.

Le registre et la cartographie nous amènent à identifier les risques et surtout établir un plan d'action. Il va falloir identifier le nombre de postes à risque : poste de secrétariat, poste de manipulateur, ceux sur lesquels sont stockées ou transitent des données.

Le plan d'action doit aussi spécifier les conditions techniques, c'est-à-dire les modalités d'anonymisation, de cryptage, de confidentialité à travers la traçabilité des consultations des données.
Des procédures doivent être mises en place pour vérifier si le système informatique est suffisamment protégé. Des tests de sécurité doivent être menés et si des failles sont constatées, il faut faire une déclaration à la CNIL. Le DPO s'en charge et doit prévenir les patients concernés d'une intrusion, par exemple, dans le système qui a mis en danger des données.

Formation des personnels

La mise en place du RGPD nécessite la formation du personnel. Lorsque le patient viendra au cabinet, il faudra que la secrétaire soit en mesure de répondre à sa demande, lui dire positivement s'il a effectivement un droit d'accès. Il faudra ensuite faire le lien avec l'informaticien si des modifications sont nécessaires.
La sensibilisation du personnel passe par sa formation. C'est en principe le rôle du DPO, quelque peu similaire à celui de la personne responsable en radioprotection sur la formation du personnel qu'elle assure tous les trois ans.

Il faudra être vigilant sur les données auxquelles secrétaires, manipulateurs, radiologues, personnels administratifs et sociétés de service peuvent avoir accès. Pour certains, seules les données administratives seront accessibles, l'accès aux antécédents du patients ne le sera pas et les données médicales seront cryptées.
Les sociétés de service, par exemple une société informatique, ne doivent pas pouvoir accéder à des données médicales des patients et encore moins en conserver dans leurs ordinateurs.

En résumé, il faut choisir un responsable DPO, commencer la rédaction du registre, informer les patients et enfin sensibiliser et former le personnel aux nouvelles règles. Il n'est pas possible de le faire du jour au lendemain mais il faut se mettre en conformité progressivement en commençant maintenant.
C'est un changement important des habitudes mais il ne faut pas oublier que l'esprit du RGPD est de protéger parce que l'on sait que les données informatiques sont une source de richesses et de commercialisation importante, à l'échelle française ou européenne.

Logiciels d'imagerie

Evolucare accompagne les radiologues vers le « tout connecté »

Les développeurs d'Evolucare Imaging n'ont pas perdu de temps pendant le confinement. Lionel Ribière, Product Manager en imagerie, nous présente les nouveaux modules connectés qui enrichissent les solutions d'imagerie de l'éditeur et répondent aux attentes des radiologues.

Lionel RIBIÈRE
Product Manager - Evolucare

Sur quelles innovations avez-vous travaillé pour 2020 ?

Lionel Ribière : Nous avons développé trois nouveaux modules connectés - prise de rendez-vous en ligne par le patient, borne d'accueil et téléradiologie. Nous avons aussi finalisé l'application mobile lancée en septembre dernier. Notre gamme imagerie se développe dans un contexte très concurrentiel, avec des éditeurs présents sur le marché depuis plus de 20 ans. Nous offrons désormais toutes les fonctionnalités indispensables pour accompagner les radiologues confrontés à de multiples enjeux, technologiques et démographiques.

La mise en œuvre d'une borne d'accueil est-elle particulièrement bienvenue en période d'épidémie ?

LR : En effet : disponible depuis le mois de juin, notre borne va aider les centres d'imagerie médicale à mettre en place les règles de distanciation devenues nécessaires pour répondre aux nouveaux enjeux sanitaires évélés par la Covid. L'automatisation de l'accueil permet de réduire les files d'attentes et de fluidifier l'arrivée des patients. Une large partie d'entre eux, maintenant familiarisée avec le numérique, utilisera la borne pour s'enregistrer par QR code ou avec une carte Vitale, et pourra imprimer les étiquettes nécessaires à son parcours dans l'établissement. Les secrétariats vont alors se consacrer aux patients qui ne sentent pas à l'aise avec la dématérialisation et aux dossiers complexes.

Dans le même esprit d'optimisation des services aux patients, vous mettez en œuvre la prise de rendez-vous en ligne...

LR : Très attendu à la fois par nos clients et par leurs patients, le module a été testé par deux premiers centres et il se révèle très facile d'utilisation. Côté patients, l'interface web est compatible avec tous les navigateurs, sur ordinateur ou téléphone mobile. Elle intègre le « captcha » de dernière génération, qui permet de sécuriser la demande en vérifiant qu'elle est bien exécutée par un humain et pas un robot. Le rendez-vous est validé après réception d'un code par SMS que le patient saisit sur son interface. Il obtient également un lien à utiliser dans le cas où il serait contraint d'annuler le rendez-vous.
Autre sécurité, côté prise de rendez-vous secrétaire : le personnel administratif voit en temps réel quand un patient sélectionne un créneau de rendez-vous, de manière à ne pas l'affecter dans le même temps à une autre demande. La solution fait gagner du temps au patient, qui n'a plus à attendre au téléphone, mais aussi aux secrétariats. En limitant les appels entrants, elle leur permet de se consacrer à un meilleur accueil sur site.
Atout supplémentaire : la possibilité d'importer l'ordonnance patient dans le dossier de prise de rendez-vous.
Au-delà de la prise de rendez-vous en ligne, nous préparons un portail patient qui offrira tous les services, de la diffusion et du stockage des comptes rendus, images, ordonnances et documents administratifs jusqu'au paiement en ligne.

La démographie professionnelle critique en radiologie conduit-elle à développer la téléradiologie ?

LR : Certaines régions rencontrent en effet des difficultés. Elles sont encouragées à utiliser des plateformes de transfert et de diffusion d'imagerie pour assurer la permanence des soins, grâce au télédiagnostic et à la téléexpertise. C'est le cas par exemple du territoire de Guadeloupe, Saint-Martin et Saint-Barthélemy, où le Groupement de Coopération Sanitaire (GCS) eSanté Archipel 971 nous a chargé en 2019 de déployer une archive territoriale[1], qui se complète d'un service de téléradiologie.
Notre offre de téléradiologie sera prête au troisième trimestre 2020, en premier lieu pour les sites équipés par Evolucare. Dans un second temps, elle s'interfacera avec d'autres systèmes d'information radiologiques. C'est ce que nous développons d'ailleurs pour le GCS.
Je précise que nous travaillons avec nos clients dans le respect complet de la charte de téléradiologie édictée par le Conseil national professionnel de radiologie et imagerie médicale (G4) et récemment réactualisée[2]. ■

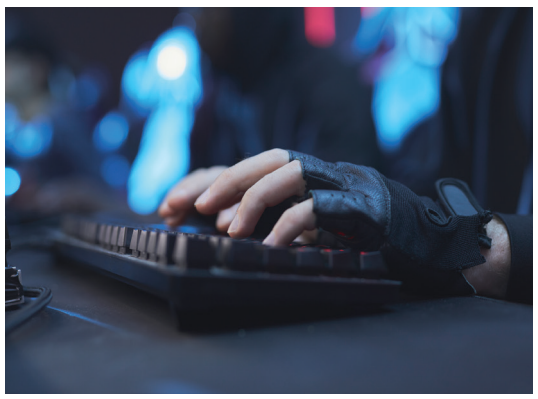
[1] Cf Le médecin radiologue – Avril 2019
[2] Disponible ici : https://frama.link/a6781UgD

Plus d'informations sur
www.evolucare.com
evolucare

Le débat[1]

> Un intervenant signale que son groupe a aussi été victime d'un ransomware introduit par un mail. Il demande au Dr A. Lesnik quel a été le point d'entrée du virus dans le système de son groupe.

Dr Alvian Lesnik. À ce jour, nous présumons, sans certitude, qu'il est arrivé par un fichier malveillant, probablement sur un CV envoyé à la DRH.
J'insiste, même si vous avez des systèmes qui fonctionnent bien, passez-les au peigne fin, un par un, vous aurez des surprises. En fait, c'est très médical. Pour que le virus, de la grippe ou autre, infecte, il faut qu'il y ait quelque part une adhérence entre la souche virale et votre corps ou votre système. Donc, si pour une raison X ou Y, vous pouvez héberger un virus de la grippe sans le développer, c'est la même chose en informatique. C'est-à-dire qu'il est possible d'être contaminé longtemps avant que le virus se développe et infecte l'ensemble du système. Nos plus anciens équipements comme les ostéo, qui peuvent avoir été infectés par des virus maintenant anciens, ont été sortis du réseau. Nous leur avons adjoint une imprimante dédiée, elle aussi extérieure au réseau.



> Quelle a été l'aide de l'État ?

Dr Alvian Lesnik. Nulle. Il faut reconnaître que les agents agissent par ordre de priorité, c'est-à-dire qu'au bout de 48 h, à partir du moment où une société du CAC 40 ou du SBF 120 est infectée, nous ne les intéressons plus. L'important pour eux est d'avoir la collection des sources virales, la façon de s'en prémunir, parce que c'est un peu la course à l'armement.
Il faut aussi savoir que certains de nos prestataires ont des accords avec une société d'antivirus. Si la base virale n'est pas à jour, certains virus ne peuvent pas être détectés et les équipements de nos prestataires deviennent des cibles potentielles.
Un intervenant invite les radiologues à être attentifs à l'informatique utilisée lors de l'acquisition de nouvelles modalités. Après avoir mis son parc à jour avec Windows 10, son cabinet a acquis, en décembre 2019, un mammographe d'une grande marque fonctionnant sous Windows 7. Mis en demeure par le cabinet de passer en Windows 10, le fabriquant du mammographe a répondu qu'il a un accord avec Microsoft pour faire évoluer les mises à jour. Le problème de sécurité reste entier.

> Christian Fortel nous a dit qu'il faut garder les données pendant dix ans. Que se passera-t-il après la perte de données provoquées par un virus ? Quel est le risque juridique ?

Dr Christian Fortel. En cas de procédure, on sait que le délai de conservation légal est de dix ans. Quand on dit dix ans, c'est dix ans après l'âge de la majorité. Il faut cumuler pour les enfants. La question qui se pose, dans ce cas de figure, est de pouvoir se défendre devant une procédure juridique. Nous disposons des comptes rendus. Auparavant, nous archivions physiquement nos clichés qui pouvaient être détruits par un incendie ou un dégât des eaux. Ce sont donc les mêmes risques qu'autrefois.

> D'une manière générale, avons-nous des assurances pour couvrir ce type de risque ou devons-nous en prendre ?

Dr Alvian Lesnik. Nous avions une assurance spécifique. Peut-être sera-t-elle plus exigeante pour de futurs contrats étant donnés les coûts. Elle imposera aussi vraisemblablement un audit.

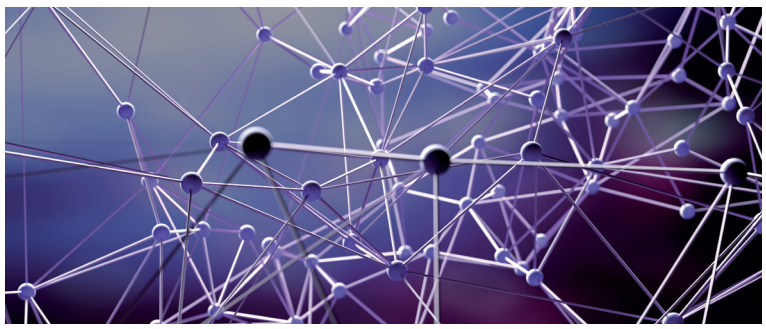
- Un intervenant confirme que son assureur sollicité pour couvrir ce type de risque a demandé un audit. Son groupe met en œuvre les recommandations de l'audit. Il a aussi décidé d'adopter un plan de restauration d'activité rapide dans la mesure où il n'est pas possible de se protéger contre tous les virus.

- Un administrateur pose la question de la prévention. Au fil de leur développement, les cabinets de radiologie font appel à des fournisseurs informatiques qui vont jouer un rôle qui n'est pas le leur, c'est-à-dire l'architecture du système. Pour la construction d'une maison, il est fait appel à des maçons, des électriciens, etc. Mais il y a avant tout un architecte. Or dans la construction des systèmes informatiques des cabinets, nous ne prenons pas d'architecte. Ce sont les fournisseurs qui vont construire par bribe l'architecture. Il faut un assistant à maitre d'ouvrage

1. Compte-rendu sous la responsabilité de la rédaction

indépendant qui sera responsable de l'architecture et imposera certaines contraintes aux fournisseurs.
De même, pour la mise en place du RGPD, il est utile de prendre un « architecte » qui fait les audits, les tests d'intrusion, etc.

Dr Alvian Lesnik. Nous n'avons pas le droit de faire des modifications sous peine d'exclusion des contrats de garantie, etc. Nous ne pouvons donc pas imposer un antivirus.



> Un radiologue demande si un Cône beam de neuf ans et demi, sous Windows 7, que son groupe possède doit être mis à l'écart du réseau et de la worklist

Dr Alvian Lesnik. Avec Windows 7, il ne sera pas possible d'être assuré. Tous les cabinets sont confrontés à ce genre de difficulté. Vous achetez une table, vous regardez si l'image est bonne, si la table descend vite et bas mais vous ne regardez pas forcément sous quelle version de Windows elle fonctionne. La table est donc récente mais son logiciel est obsolète.

> Aviez-vous une machine virtuelle qui vous aurait permis de repartir immédiatement ?

Dr Alvian Lesnik. Je ne suis pas informaticien, mais à partir du moment où tout est crypté, y compris tout ce qui est virtuel, à mon avis ça n'aurait pas apporté de solution.

- Un radiologue fait part de son expérience. Les vingt ordinateurs, y compris les plus vieux, de son cabinet sont passés de Windows 7 à Windows 10. Un seul ordinateur n'a pas pu être mis à jour. Microsoft a recommandé de le remplacer par une nouvelle machine avec une licence Windows 10. Son cabinet a adopté un système de sauvegarde sur lequel les disques sont dupliqués en Red 1. Les deux sauvegardes sont utilisées à tour de rôle. Une sauvegarde est mise à jour sur un disque, l'autre est déconnecté du réseau.

Le Dr Jean-Philippe Masson observe que, dans la plupart des cabinets, les radiologues savent qu'il est nécessaire d'investir des sommes importantes pour acquérir des équipements radiologiques de qualité. En revanche, ils peuvent hésiter à dépenser 500 € pour acheter un nouvel ordinateur supportant Windows 10 en remplacement d'une machine sous Windows 7. Les radiologues considèrent trop souvent que l'informatique est une charge. En réalité, l'informatique est devenue un outil incontournable pour les cabinets ou services de radiologie.

- Pour un autre radiologue, la vigilance doit être de tous les instants. Son groupe possède cent cinquante ordinateurs qui ont tous été homogénéisés. Ils sont en location et changés tous les trois ans. Le réseau est étanche. Il n'est pas possible de l'utiliser pour accéder à Internet. Mais récemment, lors de l'installation d'une console de lecture d'un mammographe en l'absence de l'ingénieur réseau, il a été constaté que la console ne disposait pas d'antivirus et qu'elle permettait un accès à Internet. La leçon est que la vigilance ne doit jamais se relâcher.

> Un radiologue fait part de l'exigence d'une patiente. Cette dernière, qui avait eu une échographie en vue d'une IVG, a demandé que, conformément au RGPD, son dossier soit retiré. Elle devait se marier, et pour des raisons religieuses, voulait éviter que quiconque puisse prendre connaissance de son dossier. Que faire ? La solution serait-elle de conserver un dossier papier pour respecter la règle des dix ans et de supprimer le dossier informatique ?

Dr Christian Fortel. La question est : s'agit-il de données de santé ou de données personnelles ? Chacun doit déterminer les paramètres qui conduiront à l'effacement des données. Mais dans le cas de données de santé, les médecins n'ont pas besoin d'autorisation pour les conserver ce qui paraît nécessaire en cas de procédure engagée, par exemple… par la patiente. N'oublions pas que les médecins sont tenus au secret professionnel. En revanche, le RGPD impose de mettre en place des protections pour éviter le piratage de ces données.
Alors, sur quels arguments une patiente pourrait-elle faire effacer des données ? Ce qui n'a rien à voir avec des données de santé pourra être effacé. Mais pour l'effacement des données de santé proprement dites, il faudra le motiver en fonction des critères que vous définirez dans vos registres.

> Un administrateur soulève la question des astreintes. Dans son groupe, le service informatique est en cours d'externalisation.

Préalablement, cinq sociétés ont audité le système informatique. Toutes ont relevé que les radiologues effectuaient leurs astreintes avec leurs ordinateurs portables personnels en se connectant en VPN au système informatique. Les cinq sociétés ont préconisé l'acquisition d'une flotte d'ordinateurs portables, un par associé, entièrement verrouillés et utilisés uniquement et exclusivement pour les astreintes. Aucune clé ne doit être utilisée avec ces ordinateurs.

Le Dr Jean-Philippe Masson rappelle que les examens ne peuvent être interprétés que sur des écrans adaptés et marqués CE, ce qui n'est pas le cas des ordinateurs portables.

> Les radiologues peuvent maintenant envoyer leurs comptes rendus vers le DMP[1] Quelle relation y a-t-il entre le DMP et le RGPD alors que le compte rendu est envoyé sans accord du patient ?

Dr Christian Fortel. Nous revenons à un point vu précédemment. Il s'agit de données de santé protégées par le secret médical, protégées informatiquement par un DPO.

> Quel est le pourcentage de personnes qui paient les rançonneurs ?

Dr Alvian Lesnik. Personne ne le sait. Les rançonneurs demandent beaucoup d'argent. Il y a une phase de négociation. Vous tendez un jeton pour voir. Mais avec le recul, c'est sans doute une erreur. Les informaticiens sont mobilisés pour décoder et vérifier des données alors que nous avons besoin d'eux pour remettre en route le système.
Par ailleurs, peut-on réutiliser des données qui ont été hackées ? Peut-on simplement se dire que puisque l'assurance couvre la dépense, il est possible de payer ? Mais quelle fiabilité ont ces données récupérées ? Si nous ne pouvons pas avoir confiance et si elles ne sont pas réutilisées alors il n'est pas nécessaire de négocier et de payer.
Dans le système informatique d'un groupe de radiologie, il y a 3 types d'informations stockées :
- les données comptables,
- le RIS,
- le PACS.

1. Dossier médical partagé

Deux choses sont indispensables, la comptabilité et le RIS, c'est-à-dire les données papier. Le PACS pourra être reconstitué au bout de deux ans.

Dr Alain François. Il semble qu'il y a une fixation sur Windows 7. La possession d'un poste avec Windows 7 apparaît comme un danger imminent. Inversement, la suppression de cette version assurerait la sécurité. En réalité, Windows 7 est un système fiable, sécurisé mais il ne bénéficie plus de mises à jour gratuites. Il peut être mis à jour moyennant la passation d'un contrat avec Microsoft. Si un prestataire dispose d'un tel contrat, Windows 7 reste sécurisé. Il faut seulement que le prestataire confirme par écrit qu'il bénéficie de ce contrat et que Windows 7 reste mis à jour.
Il est beaucoup question de sécurisation d'architecture, de sécurisation matérielle, de l'importance de mise à jour des modalités, des stations de travail. Mais un des points faibles d'un système informatique se situe entre la chaise et le clavier. C'est le facteur humain. On peut constater dans les centres de radiologie un manque de culture informatique tant des radiologues que des personnels. Il faut informer et former les personnels à un minimum de sécurité informatique. Ça peut se faire dans un cadre convivial, par exemple à l'occasion de la mise en place du RGPD avec, comme programme, la gestion des mails et des pièces jointes, la gestion des clés USB, fondamentale dans un groupe. Il faut aussi aborder des questions basiques comme l'interdiction de charger des téléphones portables sur les modalités en les branchant sur un port USB.
Rappelons-nous aussi que ce qui n'est pas écrit n'a pas de valeur. Il est donc utile de faire signer à chaque membre du personnel une charte informatique. C'est un bon moyen de sensibiliser le personnel et de rappeler des règles simples de gestion de leur système informatique.

> Le RGPD

Une petite structure peut confier la mise en place du RGPD à un personnel, par exemple un manipulateur. Une structure plus importante cherchera à déléguer cette fonction. Mais comment trouver la société à laquelle déléguer la mise en place du RGPD alors qu'elle doit cumuler des compétences informatiques, juridiques, voire même radiologiques ?

- Un intervenant fait part de l'expérience de son groupe qui a fait appel à une société extérieure pour l'accompagner dans le développement du RGPD mais la fonction de DPO a été confiée en interne à un radiologue.

Dr Gilbert Leblanc. Le regroupement de cabinets crée des entreprises médicales et donc des risques plus importants ce qui implique une gestion du risque.
Dans mon groupe, nous appliquons les règles de la gestion de risque de la clinique. Cela fait vingt-cinq ans que nous réalisons des tests d'intrusion. Nous avons une vraie culture du risque. Le RGPD, c'est une réglementation de plus qui est dans la case « commission des risques informatiques ».
Le risque, c'est avant tout le risque des personnels et quand on a une culture de gestion du risque, cela comprend le risque juridique, la contractualisation avec les fournisseurs. Il y a les risques en ressources humaines (RH), les risques vis-à-vis du patient, et la protection des données. Il faut donc se poser la question de recourir au cloud. Externalise-t-on ce risque et la maîtrise de la conservation des données et du secret professionnel ?
Il y a deux dimensions à ce problème. Premièrement, la gestion de base de données, donc la fragilité des données et l'interconnexion. Deuxièmement, ce sont les réseaux, c'est l'infrastructure. Par exemple, tous les radiologues qui sont dans une clinique utilisent souvent le réseau de la clinique. Notre groupe a mis deux à trois ans à sortir du réseau de la clinique. C'est plus difficile pour les cabinets qui travaillent dans un établissement appartenant à un groupe qui définit les politiques de protection pour l'ensemble des cliniques de son réseau.

La protection des cabinets de radiologie est particulièrement complexe, plus que pour les cliniciens qui consultent. Nous devons passer de la radiologie artisan à des modèles de « type industriel », même si nous ne voulons pas être industrialisés, parce que les menaces et les fragilités sont les mêmes que dans des entreprises d'autres secteurs.

> Le DPO

Pour le Dr Christian Fortel le DPO peut être en interne, par exemple un manipulateur, et Maître Méot nous dit qu'il doit être indépendant. Quel choix faire ?

Maître Méot répond que la réglementation prévoit qu'il peut être désigné en interne ou en externe, mais dans tous les cas, il doit être indépendant. C'est-à-dire que si c'est un DPO interne, il faut prévoir une organisation de son travail, de son statut pour faire en sorte qu'il soit indépendant. C'est pour ça que du point de vue de la réglementation, dans une structure d'assez petite taille, je trouve qu'il est difficile d'être conforme aux principes du RGPD sur ce sujet en nommant un DPO interne. Il est vrai que dans une plus grosse entreprise, il y a des dissolutions de la responsabilité et du pouvoir. De ce fait, il est plus facile à un service interne d'être indépendant. Mais d'un autre côté, comme on veut aussi que le DPO soit compétent dans le domaine d'intervention et que la radiologie est un domaine très spécifique, il est tentant de prendre un prestataire interne. Donc, en soi, les deux sont possibles et c'est seulement, à mon sens, le prestataire externe, du point de vue de l'indépendance, qui correspond le mieux à ce que prévoit le texte.

> Un intervenant fait remarquer qu'il y a un petit risque à prendre un DPO en interne, comme dans le cas de la PCR[2]. Si l'on désigne un manipulateur ou un cadre comme DPO, le jour où il y a un conflit ou s'il s'en va, il n'y a plus de DPO et tout à refaire

Dr Jean-Philippe Masson. Il est sans doute plus facile de former un DPO que de former un PCR. N'oublions pas qu'il y a dans Labelix un volet sécurité informatique et un volet RGPD.

- Un administrateur indique que son groupe, labelisé Labelix, a mis en place le RGPD dans ce cadre faute de quoi il n'aurait pas pu conserver son label.

> Les accidents de cybersécurité doivent être déclarés à la CNIL. Il y a des services de gendarmerie qui sont spécialisés dans la cybersécurité. Les préfectures ont des antennes pour la cybersécurité. Alors que font les services de l'État hormis le recueil de données ?

Dr Alvian Lesnik. Nous avons fait la déclaration à la CNIL. Il y a un temps de latence entre la déclaration et la remontée de l'information au niveau national. Il faut reconnaître, qu'au début, lorsque nous allons à la gendarmerie, nous ne sommes pas pris au sérieux. Mais au bout de deux jours, nous avons reçu des appels venant « d'en haut ». Les appelants ne donnent ni leur nom, ni leur qualité, ni le nom de leur administration. Dans notre expérience, ce n'est d'ailleurs pas à nous, les radiologues, qu'ils veulent parler mais aux informaticiens. Ensuite, les appels cessent et il ne se passe plus rien.

2. Personne compétente en radioprotection

Le président conclut la journée en rappelant qu'il avait invité, depuis plusieurs mois, pour qu'ils participent à ce séminaire, les services de l'État et en particulier l'ANSSI[3] mais ils ont dit ne pas être disponibles. Manifestement, ils ne souhaitaient pas participer.
Enfin, il remercie l'URPS AURA[4] pour les fiches sur la sécurité informatique que l'Union a distribuées aux participants du séminaire. Elles seront téléchargeables sur le site de la FNMR.

3. Agence nationale de la sécurité des systèmes d'information
4. Union régionale des professionnels de santé – Auvergne Rhône Alpes

RGPD

Règlement Général sur la Protection des Données personnelles

URPS médecins libéraux Auvergne Rhône Alpes

Les six points européens

- Redéfinition du consentement
- Des données supprimées lorsqu'elles deviennent obsolètes
- Minimisation et restriction du traitement des données
- Intégrité des données
- Confidentialité
- Risques encourus en cas de non-respect du Règlement

Les obligations des médecins

- **Le dossier médical** : Respecter les obligations de fond, mettre en place un **registre** (exemple : https://bit.ly/2LrGmJS), sécuriser l'accès aux données, veiller à la durée de conservation des données...
- **La prise de rendez-vous** : Mêmes obligations que pour les dossiers (limitation du recueil d'informations, tenue à jour des traitements).
- **La messagerie électronique** : Utiliser les messageries sécurisées lors des échanges d'informations avec les professionnels de santé.
- **Les smartphones et tablettes** : Veiller à ce que l'accès aux applications médicales soit sécurisé, éviter de stocker des données sur ces outils.
- **La télémédecine** : Toute séance de télé-consultation doit passer par des outils sécurisés.
- **Les objets connectés** : S'interroger sur le cryptage, l'hébergement et la sécurisation de ses accès, le traitement des données...

Pour en savoir plus, consultez le site de l'URPS Médecins
[CYBERSÉCURITÉ] ET [RGPD] http://bit.ly/2tuPZ2y

Consultez et téléchargez les fiches d'alerte gendarmerie disponibles à cette adresse :
www.12h15.fr/se-proteger

urps@urps-med-aura.fr

URPS Médecins Libéraux Auvergne-Rhône-Alpes
20, rue Barrier 69006 LYON ~ 04 72 74 02 75
24, allée Évariste Galois 63170 AUBIÈRE ~ 04 73 27 77 44

Jean-Jacques ZAMBROWSKI, délégué général
de la Société française de santé digitale (SFSD)

Un défi stratégique pour le système de santé

Délégué général de la Société française de santé digitale, Jean-Jacques Zambrowski détaille les multiples enjeux liés à la cybersécurité, qu'il considère comme une priorité stratégique dans le domaine de l'imagerie médicale. Selon lui, les défis sont sanitaires, économiques, technologiques, mais aussi juridiques. Il réclame notamment des sanctions exemplaires à l'encontre des hackers.

DR

Jean-Jacques ZAMBROWSKI

> Pourquoi le secteur de la santé est-il de plus en plus souvent visé par des cyberattaques ?

La cybersécurité exige des moyens humains, techniques et économiques conséquents. À l'exception de certains grands groupes hospitaliers, le secteur de la santé n'est pas préparé à ces attaques, à la différence du secteur bancaire, bien mieux armé. Les données de santé sont une mine d'or pour les hackers. Elles peuvent être facilement revendues à des opérateurs peu scrupuleux, capables de les exploiter à des fins mercantiles. Faute d'un niveau de protection suffisant, les établissements de soins et les cabinets de radiologie sont malheureusement des cibles privilégiées.

> En quoi les cabinets de radiologie sont-ils particulièrement exposés ?

Les diagnostics et les comptes-rendus médicaux ont une valeur inestimable pour des personnes mal intentionnées. En radiologie, l'analyse, le stockage et la transmission des informations sont des enjeux majeurs, parfois vitaux. Cette profession ne peut pas fonctionner sans un système informatique fiable et opérationnel. En cas de problème, elle pourrait être indirectement tenue responsable des dommages causés par un hacker.

> Pour quelles raisons ?

Dans la plupart des cas, la décision médicale du radiologue repose sur l'interprétation d'images. Si les données analysées sont falsifiées, son jugement peut être altéré, dans le bon comme dans le mauvais sens. Sans le vouloir, il peut mettre la santé de son patient en danger. Les cabinets de radiologie doivent déployer tous les moyens nécessaires pour se protéger efficacement. L'émergence des nouvelles technologies renforce d'autant plus ce besoin, tant elles démultiplient les facteurs de risque.

> C'est-à-dire ?

D'une certaine manière, le domaine de l'imagerie médicale est victime de son succès. Il concentre les principaux développements algorithmiques, avec les meilleures perspectives de résultats. L'intelligence artificielle est une arme à double tranchant pour les radiologues. C'est un levier efficace pour accroître la précision du diagnostic, mais c'est aussi une porte d'entrée pour les hackers, qui profitent allègrement du tout numérique pour prospérer. Leur mode opératoire est connu de tous.

> Quelles sont leurs méthodes ?

Ils paralysent les systèmes informatiques d'un groupe hospitalier, d'un établissement de santé ou d'un cabinet de radiologie libérale. Ils peuvent subtiliser des données médicales sensibles sur les patients. Ils peuvent truquer les images produites par tous les équipements radiographiques, scanner et IRM compris. Ils peuvent altérer le processus de transmission des informations essentielles à la prise en charge. Leur pouvoir de nuisance est énorme.

> Quelles sont les motivations des hackers ?

Pour débloquer la situation, ils exigent généralement des rançons importantes, sous la forme de bitcoins. Cette monnaie virtuelle échappe à toute forme de traçabilité, raison pour laquelle elle est souvent privilégiée par les

cybercriminels. Certains vont même jusqu'à réclamer de l'argent, en échange d'une protection informatique. Ces sont des méthodes mafieuses, ni plus ni moins.

> Quelle est la fréquence de ces attaques ?

La fréquence est très élevée. Selon le service ministériel de traitement des signalements mis en place il y a un peu moins de trois ans, on dénombre une cyberattaque en moyenne par jour, avec des cibles bien identifiées (voir encadré). Le groupe OrangeWorm est particulièrement actif dans le secteur de la santé. À lui seul, il est responsable de 40% des « agressions » répertoriées.

> Quel est le cas le plus significatif enregistré à ce jour ?

L'été dernier, Ramsay-Générale de Santé a été victime d'une attaque virale d'une ampleur inédite. Les 120 établissements français du groupe spécialisé dans l'hospitalisation privé ont été touchés. Le système de messagerie et plusieurs applications professionnelles ont été totalement paralysés, condamnant le personnel à l'usage du papier et du crayon pour la gestion des tâches courantes, comme l'organisation des plannings ou la prise de rendez-vous.

CYBERATTAQUES : LES CHIFFRES-CLÉS

Nombre de cyberattaques signalées : 478

Établissements de santé : 88%

Établissements d'hébergement pour personnes âgées dépendantes : 6%

Laboratoires de biologie médicale : 4%

Centres de radiothérapie : 2%

NB : Période allant du mois d'octobre 2017 au mois d'avril 2019

SOURCE : ASIP SANTÉ (MAI 2019)

> Quels ont été les dommages subis ?

Il aura fallu plusieurs jours pour restaurer l'intégrité des serveurs, dont les données avaient été cryptées. La crise a été gérée de façon efficace, puisqu'aucune information sensible n'a pu être exfiltrée. De la même manière, aucune répercussion dommageable sur la santé des patients n'a pu être directement reliée à cet événement. Cet incident nous rappelle néanmoins à la réalité : personne n'est à l'abri !

> Quels sont les risques en matière de santé publique ?

Ces cyberattaques peuvent désorganiser une structure hospitalière toute entière. Elles peuvent surtout mettre en péril la santé des patients. Interprétation du résultat, diagnostic, protocole de soins : toutes les étapes de la chaîne de décision médicale peuvent être impactées, avec des conséquences non négligeables sur la coordination de la prise en charge et la continuité des soins. Aucun incident dramatique n'est pour l'instant à déplorer, mais il ne faudra pas attendre de compter les morts avant de réagir.

> Comment les acteurs de santé peuvent-ils se prémunir de ces attaques ?

Les hackers s'attaquent plus facilement aux systèmes fragiles et vulnérables. La plupart des grands groupes hospitaliers ont pris conscience de la chose, à l'image de l'AP-HP[1]. Ils ont su déployer des services informatiques entièrement dédiés à la cybersécurité. Ce n'est pas une garantie absolue, mais c'est un prérequis indispensable pour atténuer le risque. La FNMR s'est également emparée du sujet, il y a de nombreuses années.

> Quelles sont vos recommandations ?

C'est d'abord une question de maturité et de conscience du danger. Peu importe leur taille, les acteurs de santé doivent absolument investir pour améliorer la gestion de leurs données sensibles. À défaut, ils doivent s'adosser à des opérateurs spécialisés pour protéger leurs infrastructures. Les cabinets de radiologie ne dérogent pas à la règle, bien au contraire. La cybersécurité n'a pas de prix.

> Quel appui la Société française de santé digitale peut-elle leur apporter ?

Nous sommes un relais auprès des autorités compétentes, comme la CNIL[2], l'ANSSI[3] ou l'ANS[4]. Nous participons activement à la surveillance, à la signalisation et à la résolution des incidents, mais aussi à l'élaboration de

1. Assistance Publique – Hôpitaux de Paris
2. Commission nationale de l'informatique et des libertés
3. Agence nationale pour la sécurité des systèmes d'information
4. Agence du numérique en Santé

recommandations thématiques, inhérentes à la protection des données. Nous accompagnons par ailleurs le déploiement du volet numérique du plan « Ma Santé 2022 », qui prévoit notamment la création d'un service national de cybersurveillance en santé.

Il faut légiférer sur la cybercriminalité de façon brutale et dissuasive.

> Faut-il renforcer les sanctions à l'encontre des cybercriminels ?

Bien évidemment. Les hackers bénéficient d'une longueur d'avance, parce qu'ils utilisent des moyens techniques ultrasophistiqués et intraçables. Ils sont malheureusement très difficiles à débusquer. Ils profitent également d'un vide juridique pour opérer en toute impunité, abusant parfois de certaines législations laxistes ou incomplètes. L'arsenal répressif est aujourd'hui insuffisant. Il faut impérativement légiférer sur cette problématique, de façon brutale et dissuasive.

> Quelles sont vos préconisations en la matière ?

La cybercriminalité dans le domaine de la santé doit être considérée comme une circonstance aggravante. Il convient d'adopter des sanctions exemplaires à l'encontre des hackers, et le faire savoir. La complicité de meurtre, voire le meurtre avec préméditation, serait un chef d'accusation tout à fait légitime. À tout le moins, une lourde amende et une peine de prison significative seraient un compromis acceptable, au regard des risques encourus par les patients. Une chose est sûre, la réponse juridique ne pourra pas être uniquement franco-française. Il appartient à l'Europe de se prononcer sur cette question cruciale.

Propos recueillis par **Jonathan ICART**

Pr Jean-Nicolas DACHER, responsable du pôle imagerie médicale du CHU de Rouen

Une vigilance de chaque instant

Jean-Nicolas Dacher analyse les conséquences de la cyberattaque dont le CHU de Rouen a été victime il y a quelques mois. Il rappelle les enjeux liés à la protection des données de santé, livrant au passage quelques recommandations pratiques. Selon lui, il faut engager des moyens humains, techniques et financiers importants pour garantir la sécurité des patients.

DR

Pr Jean-Nicolas DACHER, médecin radiologue

> Votre établissement a récemment été victime d'une attaque informatique. Comment les hackers ont-ils procédé ?

Le 15 novembre dernier, le CHU de Rouen a été infecté par un « ransomware ». Ce logiciel malveillant a crypté l'ensemble des données auxquelles il a pu avoir accès. Tous les ordinateurs allumés ont été parasités, soit les trois-quarts de notre parc informatique. Les périphériques de stockage externes restés branchés ont également été contaminés. Les hackers réclamaient une somme d'argent significative pour déverrouiller chaque poste. L'attaque s'est produite un vendredi, en fin de journée, vers 18h00. Un moment à haut risque, parce qu'il coïncide généralement avec la fermeture des bureaux et les départs en week-end.

> Comment la crise a-t-elle été gérée ?

Le directeur général de l'établissement a immédiatement déclenché un « plan blanc ». Une cellule de crise a rapidement été constituée, avec le directeur des systèmes d'information. Nous avons également reçu le précieux concours de l'ANSSI[1], le service de cybersécurité rattaché au ministère de l'Intérieur. Les agents mobilisés ont fait preuve d'un professionnalisme et d'une efficacité hors pair. Ils ont travaillé sans relâche pour résoudre l'incident. Preuve de la violence de l'attaque, il aura fallu attendre vingt-cinq jours pour rétablir la situation.

1. Agence nationale de la sécurité des systèmes d'information

> Le service de radiologie a-t-il été touché ?

Naturellement. Peu ou prou, tous les patients transitent par le service de radiologie. C'est le centre névralgique d'un hôpital. Les systèmes d'archivage des images et des comptes-rendus représentent une mine d'or pour des personnes mal intentionnées. Je n'ai pas été attaqué personnellement, parce que j'avais pris mes précautions. Certains de mes collègues n'ont pas eu cette chance.

> Quelles ont été les conséquences de l'attaque sur le fonctionnement du CHU ?

Il y a eu des répercussions organisationnelles dommageables. Plusieurs applications professionnelles ont été totalement paralysées. Nous avons notamment été contraints de revenir au papier et au crayon pour des activités essentielles, comme la gestion des plannings ou la programmation des rendez-vous. Nous avons également coupé l'Internet pendant un long moment pour éviter d'éventuelles répliques, quitte à nous priver de certains outils utiles pour optimiser la prise en charge des patients. Malgré tous nos efforts, nous avons perdu de nombreuses données.

> Lesquelles ?

Des analyses biologiques, des images radiographiques, des résultats d'examens et des comptes-rendus médicaux, soit un grand nombre d'informations contenues dans des dossiers patients, que nous n'avons pas pu tous sauver de la destruction, au détriment de l'intérêt général. Dans la précipitation, certains utilisateurs ont effacé les fichiers corrompus. Ceux qui les ont conservés ont finalement pu les récupérer, quelques semaines plus tard.

> Y a-t-il eu des dommages collatéraux sur le plan sanitaire ?

Aucun accident majeur n'est à déplorer : aucun pillage de données ni aucun décès n'ont pu être directement reliés à la panne. Tout le processus de la décision médicale a

néanmoins été impacté. La coordination et la continuité des soins ont été mises en péril, au même titre que la santé des patients. Cet incident aurait très bien pu mal tourner…

> À la faveur de votre expérience, quels conseils pratiques pouvez-vous donner ?

Verrouillez votre session et éteignez systématiquement votre ordinateur avant de quitter votre lieu de travail, qui plus est en fin de semaine ! N'oubliez pas non plus de débrancher vos disques durs externes, si vous n'en n'avez pas l'utilité. Pensez surtout à stocker vos données sur un serveur sécurisé, comme un NAS. Une double sauvegarde n'a rien de superflu. Ce sont des mesures préventives assez simples, mais très efficaces.

Dans le domaine de la santé, la sécurité informatique n'a pas de prix

> Quels sont les principaux enjeux liés à la cybersécurité ?

La cybersécurité recoupe de nombreux enjeux, à commencer par la protection de la vie privée. Les données de santé sont des informations à caractère personnel qui ne doivent pas être divulguées. Légalement, les structures de soins sont responsables de leur traitement. Les hôpitaux sont sur-informatisés. N'importe quelle attaque peut avoir des conséquences organisationnelles et sanitaires dramatiques. Il faut engager des moyens humains, techniques et financiers importants pour garantir la sécurité des patients. La détection des spams, des e-mails et des logiciels frauduleux est un défi de chaque instant.

> Les cabinets de radiologie médicale sont-ils également concernés ?

Dans les cabinets de radiologie médicale, la gestion des systèmes d'information est parfois très aléatoire. Ils ne disposent pas toujours de consultants informatiques attitrés. Quelle que soit sa taille, chaque établissement doit impérativement se prémunir des intrusions externes et des attaques par « rançongiciel ». En conséquence, il doit se doter de services dédiés, et recruter des profils qualifiés et expérimentés. Au-delà des questions de responsabilité, c'est l'intégrité du diagnostic qui est en jeu. Le stockage et la transmission des données sont également des paramètres déterminants. Ce sont des enjeux stratégiques majeurs pour la profession, mais aussi pour les patients.

> Quelles sont les motivations des hackers ?

Leurs intentions sont claires : ils cherchent à extorquer des fonds ou à exfiltrer des données sensibles pour les revendre aux plus offrants, la plupart du temps sur des marchés clandestins. Ils sollicitent des modes de paiement virtuels, souvent intraçables, à l'image des bitcoins. Le secteur de l'imagerie médicale est un « marché » particulièrement lucratif pour les pirates informatiques.

Il existe des mesures préventives assez simples, mais très efficaces.

> Le développement de l'intelligence artificielle majore-t-il le risque ?

Assurément. Certaines sociétés spécialisées tentent de récupérer des données pour entraîner leurs algorithmes, quitte à employer des méthodes peu conventionnelles. Les hackers l'ont bien compris. Les grands groupes constituent d'ailleurs une cible privilégiée, parce qu'ils disposent d'une banque d'images fournie et de comptes-rendus médicaux documentés, qui contribuent à enrichir la connaissance de la « machine ». Combinées, ces données sensibles ont une valeur inestimable. La menace est considérable.

COVID-19 : GARE AUX VIRUS INFORMATIQUES !

Pas de répit, même en pleine crise sanitaire. Selon l'ANS[1], les hackers utilisent le prétexte du Covid-19 pour répandre un autre genre de virus. « Via de faux e-mails des autorités de santé, de fausses notes internes ou encore de fausses alertes quant à des retards de livraison, les cybercriminels tentent d'exploiter la peur liée à la pandémie pour s'infiltrer sur les réseaux informatiques des entreprises et des particuliers », souligne-t-elle. L'ANS recommande notamment de « surveiller de près tout élément anormal » dans les systèmes d'information et de « faire un signalement immédiat », le cas échéant. Elle suggère également de « vérifier le bon fonctionnement des sauvegardes » et de « sensibiliser l'ensemble des personnels ». Elle préconise surtout de « ne pas cliquer sans vérification préalable sur les liens de ces messages ni sur leurs pièces jointes ».

1. Agence du numérique en santé

> Comment les établissements de santé et les cabinets de radiologie peuvent-ils se prémunir de ces attaques ?

Mise en conformité, prévention, surveillance, signalement, gestion de crise : une série de mesures proposées par les pouvoirs publics permettent de faire face à l'extrême diversité des risques. Des bonnes pratiques, des guides d'information et des outils techniques sont à la disposition de toutes les structures de santé. Elles doivent s'en saisir, et faire le nécessaire. Une chose est sûre, il vaut mieux prévenir que guérir, quoi qu'il en coûte. Dans le domaine de la santé, la sécurité informatique n'a pas de prix. Dans notre pôle imagerie, nous avons une cellule active, avec trois personnes à temps plein.

> Faut-il renforcer les sanctions à l'encontre des cybercriminels ?

Il faut déjà pouvoir les trouver ! Ils emploient traditionnellement des méthodes intraçables. Ils profitent également d'un vide juridique pour prospérer en toute impunité. Ils agissent souvent depuis l'étranger, échappant ainsi à la juridiction française. La problématique doit être appréhendée à l'échelon international. Il convient d'adopter des sanctions exemplaires et réellement dissuasives dans tous les pays du globe.

Propos recueillis par **Jonathan ICART**

uniprévoyance

Santé et Prévoyance, Action sociale et Services, nous avons tant à partager

SANTÉ • PRÉVOYANCE

Votre protection sociale, c'est notre métier !

Pour toute information : contact@uniprevoyance.fr

www.uniprevoyance.fr

Dr Jacques LUCAS, président de l'Agence du numérique en santé – ANS
Emmanuel SOHIER, responsable de la cellule Accompagnement cybersécurité des structures de santé de l'ANS

Recommandations de l'Agence du Numérique en Santé face aux cyberattaques

La cybercriminalité est devenue depuis plusieurs années une menace importante pour toutes les structures de santé : crypto-virus, hameçonnage, pouvant aboutir à la perversion ou la perte de données avec un risque de mise en danger dans la prise en charge des patients et à des demandes de rançon pour les structures paralysées dans leurs fonctionnements.


DR

Dr Jacques LUCAS


DR

Emmanuel SOHIER

Le manque de vigilance ou la méconnaissance des techniques d'attaque permettent à des pirates de récupérer des identifiants de comptes de messagerie ou de déployer des rançongiciels au sein des systèmes d'information. **Il est donc essentiel que toutes les structures de santé poursuivent leurs efforts en matière de sensibilisation des médecins et leurs personnels concernant cette menace.** Tous les utilisateurs doivent être informés de l'importance :
- de la sécurité de leurs mots de passe ;
- de savoir identifier les messages électroniques frauduleux ;
- d'éviter d'utiliser des supports de stockage personnels ou de télécharger des fichiers sur leur poste de travail.

Sur sa plateforme de formation e-santé (https://esante-formation.fr), l'Agence met à disposition gratuitement des vidéos de sensibilisation rappelant les bonnes mesures d'hygiène numérique. Ces supports sont présents sous la thématique « Sécurité opérationnelle des SI » et sont accessibles après avoir créé préalablement un compte d'accès.
Si elle est victime d'une attaque de grande ampleur, il est essentiel pour la structure de pouvoir disposer de sauvegardes pour restaurer les données. Il est donc fortement recommandé de gérer des sauvegardes hors ligne, afin d'avoir l'assurance de disposer de sauvegardes intègres en cas de compromission majeure du système d'information.

Des fiches réflexes selon le type de l'incident sont à disposition sur le portail cyberveille-santé (https://www.cyberveille-sante.gouv.fr).

Elles rappellent les bonnes pratiques en matière de prévention et de réaction face aux principales menaces. Grâce au portail cyberveille-santé, les acteurs opérationnels de la sécurité sont informés quotidiennement des vulnérabilités et des dysfonctionnements majeurs impactant des dispositifs médicaux, des logiciels de santé ou des logiciels standards (système d'exploitation, suite bureautique, base de données, etc.). Il diffuse aussi régulièrement des alertes sur des actes de cyber malveillance (campagne de messages électroniques malveillants, crypto-virus, vols de données, etc.).

Le dispositif de traitement des signalements des incidents de sécurité des systèmes d'information

https://www.cyberveille-sante.gouv.fr

constitue un élément clé de la stratégie d'amélioration du niveau de sécurité numérique du secteur santé. Sa mise en œuvre opérationnelle s'appuie sur la cellule Accompagnement cybersécurité des structures de santé (ACSS) de l'Agence du numérique en santé (ANS). La cellule ACSS (cyberveille@sante.gouv.fr) propose une démarche méthodique pour améliorer la résilience des structures face aux actes de cyber malveillance. Un service support téléphonique va être prochainement mis en place.

Lorsqu'elles déclarent leur incident de cybersécurité sur le portail des événements sanitaires indésirables (https://signalement.social-sante.gouv.fr) en allant sur l'espace « Professionnel de santé », les structures de santé sont notifiées de la prise en compte de leur signalement et peuvent bénéficier d'un appui concret de la cellule ACSS dans :
- les actions visant à limiter l'effet ou la portée de l'incident (isoler les machines concernées, bloquer les comptes compromis, bloquer les accès à distance, etc.) ;
- la recherche de l'origine de l'incident et de l'activité malveillante (phishing, maliciel) afin de mettre en place des mesures de remédiation pour se protéger contre une nouvelle occurrence (analyse de messages de hameçonnage, de souches virales, de fichiers chiffrés, de journaux système) ;
- la mise en place de mesures de remédiation et d'amélioration de la sécurité (administration des systèmes, gestion de l'Active Directory (annuaire), renforcement de la politique de contrôle des messages et flux webs malveillants).

L'agence régionale de santé (ARS) territorialement compétente et le Fonctionnaire de Sécurité SI des ministères sociaux sont systématiquement informés des actions d'accompagnement menées auprès des structures. Dans le cas d'un incident ayant un impact sanitaire, la cellule ACSS diffuse une alerte à la direction générale de la santé (DGS) via le CORRUSS (Centre opérationnel de réception et de régulation des urgences sanitaires et sociales).

Le ministère de la santé et l'ANS mettent progressivement en place un service de cybersurveillance des structures de santé exposées sur Internet afin de détecter d'éventuelles vulnérabilités. **Ce service opéré par l'ANS permet aux structures de renforcer la sécurité opérationnelle de leurs systèmes numériques et contribue à garantir la confiance dans la e-santé (action 9 de la feuille de route « Accélérer le virage numérique » de « Ma Santé 2022 »).** Sa mise en œuvre a permis à de nombreuses structures de réduire les risques de compromission de leur SI au travers de leurs services numériques accessibles via Internet.

Armelle GRACIET, directeur des affaires industrielles – SNITEM[1]

Prise en compte par les industriels de la sécurité face aux attaques informatiques dans les modalités vendues aux radiologues

L'augmentation exponentielle du volume et des types de données disponibles entraîne inévitablement une vulnérabilité accrue à la cybercriminalité et les appareils d'imagerie ne sont pas à l'abri de ce genre de cyberattaques. C'est pourquoi les industriels de l'imagerie se sont engagés à déployer des plans de sécurité complets qui garantissent la sécurité des produits, des données personnelles des patients et des données de leurs clients professionnels et établissements de santé et ce, dès la conception et le développement des produits.


DR

Armelle GRACIET

L'augmentation exponentielle du volume et des types de données disponibles entraîne inévitablement une vulnérabilité accrue à la cybercriminalité.

Les données relatives aux soins de santé sont la cible numéro un des cybercriminels et ont dix fois plus de valeur que les seules données relatives aux cartes de crédit. Les données personnelles contenues dans les dossiers médicaux sont très précieuses, car elles peuvent être utilisées à des fins malveillantes comme la création de fausses identités ou de fausses demandes d'assurance. Les menaces comprennent les attaques de sécurité malveillantes via des virus, des worms et le hacking.

Deux milliards de dossiers personnels ont été volés aux États-Unis en 2016, dont 100 millions de dossiers médicaux et la cybercriminalité a coûté à l'économie mondiale plus de 450 milliards de dollars en 2016. Le coût de la cybercriminalité était estimé à 2000 milliards de dollars en 2019.

Les appareils d'imagerie ne sont pas à l'abri de ce type de cyberattaques. La plupart a été développée en mettant l'accent sur l'utilité clinique, sans tenir compte du fait qu'il s'agit également d'ordinateurs sur un réseau qui peut être exploité à des fins illégales. Les dispositifs médicaux sont donc vulnérables et les hackers peuvent utiliser ces dispositifs médicaux fermés comme des points de pivot dans le système de santé. Une stratégie de sécurité cohésive de défense en profondeur peut aider les prestataires de soins de santé à éviter les failles de sécurité à l'avenir.
Conscients des préoccupations de leurs clients et des patients, et du rôle essentiel que joue la sécurité dans les écosystèmes numériques interconnectés d'aujourd'hui, les industriels de l'imagerie se sont engagés à déployer des plans de sécurité complets qui garantissent la sécurité des produits, des données personnelles des patients et des données commerciales (informations d'entreprises). Ils encouragent l'adoption cohérente de stratégies pour faire face de manière proactive aux risques et aux menaces, y compris ce que l'on appelle souvent dans le domaine de la cybersécurité les « trois péchés capitaux » :
- le risque lié aux mots de passe : le risque lié à l'absence d'une gestion solide des identités et des autorisations, par exemple l'authentification multifactorielle,
- le risque de cryptage : risque lié à l'absence d'un cryptage solide des données de bout en bout – de la source où les

1. Syndicat national de l'industrie des technologies médicales

données sont générées, sur le réseau et lorsqu'elles reposent dans un centre de données– et/ou de solutions efficaces de prévention des pertes de données,
- le risque de gestion des correctifs : risque lié à l'absence d'une gestion efficace des correctifs, créant des vulnérabilités dans les systèmes d'exploitation existants, par exemple.

Les entreprises mettent en œuvre la sécurité dans un secteur des dispositifs médicaux déjà fortement réglementé. Les organismes de réglementation tels que la Food and Drug Administration américaine exigent que les versions et les modifications de matériel et de logiciels soient soumises à des méthodes de vérification et de validation rigoureuses afin de garantir le respect de normes élevées de sécurité, de sûreté, d'efficacité, de qualité et de performance dans tous les produits et services.

Les entreprises sont en permanence à l'affût des nouvelles vulnérabilités en matière de sécurité et des menaces externes potentielles, mais elles collaborent également avec les agences de régulation, les partenaires industriels et les prestataires de soins de santé pour combler les lacunes en matière de sécurité et mettre en place des mesures de protection.
L'intégration des principes de sécurité commence dès la conception et le développement des produits, jusqu'au déploiement en passant par de nombreux tests. Elle est suivie de politiques et de procédures solides pour le suivi, de mises à jour efficaces et, si nécessaire, de la gestion des réponses aux incidents.

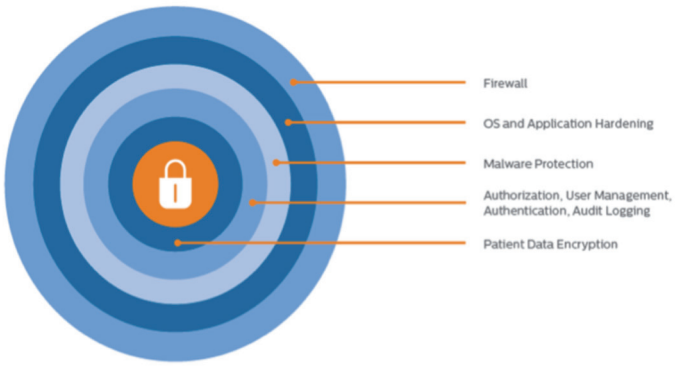


*SCHÉMA FOURNI PAR PHILIPS FRANCE

Les entreprises mettent en œuvre des normes de sécurité qui respectent, voire dépassent, les exigences réglementaires actuelles et les meilleures pratiques du secteur.

Elles surveillent le marché et répondent aux menaces, vulnérabilités et incidents de sécurité en les surveillant en permanence y compris les vulnérabilités identifiées par les fournisseurs de systèmes d'exploitation et d'autres logiciels tiers, ainsi que par les clients et les chercheurs en sécurité. Les équipes de réponse aux incidents de sécurité des entreprises évaluent les incidents de sécurité potentiels et les vulnérabilités découvertes et élaborent des plans de réponse si nécessaire.
Elles assurent également la protection contre les logiciels malveillants et la gestion des correctifs :
• Les produits qui prennent en charge la protection contre les logiciels malveillants disponibles dans le commerce sont livrés avec un logiciel de protection contre les logiciels malveillants préinstallé ou avec une documentation client détaillant les paramètres de protection contre les logiciels malveillants spécifiques au produit.
• Les produits peuvent utiliser des logiciels tiers, y compris des systèmes d'exploitation comme Microsoft Windows et Linux. Les évaluations d'impact de ces correctifs par les équipes d'ingénierie commencent généralement dans les 48 heures suivant la prise de conscience par l'entreprise d'une nouvelle vulnérabilité de sécurité ou de la disponibilité d'un correctif.

CNIL. **Marie-Laure DENIS,** présidente de la Commission nationale de l'informatique et des libertés – CNIL

Respectez les bonnes pratiques !

Selon la présidente de la CNIL, les organismes liés au secteur de la santé sont confrontés à de nouveaux enjeux en matière de protection des données à caractère personnel. Marie-Laure Denis rappelle la conduite à tenir pour améliorer le niveau de sécurité des infrastructures informatiques. Elle liste notamment une série de mesures préventives visant à réduire les facteurs de risque.


DR

Marie-Laure DENIS

> Les structures de santé sont de plus en plus souvent ciblées par les cybercriminels. Quelles sont aujourd'hui les données les plus sensibles ?

Particulièrement sensibles, les données de santé doivent impérativement être protégées par ceux qui sont responsables de leur traitement. Selon le RGPD[1], il s'agit « des données relatives à la santé physique ou mentale d'une personne physique qui révèlent des informations sur l'état de santé de cette personne ». La prestation de soins s'inscrit naturellement dans ce champ. Très large, la notion doit néanmoins être appréciée au cas par cas, en fonction de la nature des données recueillies.

> En quoi le secteur de l'imagerie médicale est-il particulièrement concerné ?

La règlementation est limpide : les données anonymisées restent des données de santé à caractère personnel, quand bien même elles ne comportent aucun nom, prénom ni aucune date de naissance. Dans les cabinets de radiologie médicale, les images produites sont souvent associées à de nombreuses métadonnées relatives aux patients. En cas de divulgation, elles représentent un risque accru pour la vie privée.

> En matière de protection des données, quelles sont les obligations imposées aux structures de santé ?

Toujours selon le RGPD, le responsable de traitement et le sous-traitant doivent « mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ». Un risque souvent élevé quand on « manipule » des données de santé. Outre le RGPD, d'autres textes juridiques sont également applicables. Pour certains cas décrits dans le Code de la santé publique[2], l'hébergement des données de santé peut notamment nécessiter le recours à un sous-traitant agréé ou certifié.

> En cas de non-respect de la réglementation, quelles sont les sanctions prévues ?

Les autorités en charge de la protection des données ont la capacité de sanctionner les contrevenants. Deux mois après l'entrée en vigueur du RGPD, l'équivalent portugais de la CNIL – le CNPD – a infligé une amende de 400 000 euros à l'hôpital de Barreiro, après avoir relevé plusieurs manquements dans les procédures de gestion des données personnelles, notamment en matière d'accès.

> Quels ont été les motifs retenus pour justifier la sanction financière ?

La non-désactivation des comptes inactifs ou appartenant à des personnels qui ne travaillaient plus dans l'établissement, l'absence d'une procédure indiquant les règles à suivre pour la création d'un compte, l'attribution d'accès et l'attribution de privilèges ou encore l'absence de niveaux d'habilitation pour l'accès aux dossiers patients informatisés. Toutes les règles édictées dans le RGPD doivent être

1. Règlement général sur la protection des données
2. Articles L. 1111-8 et R. 1111-8-8 du code de la santé publique

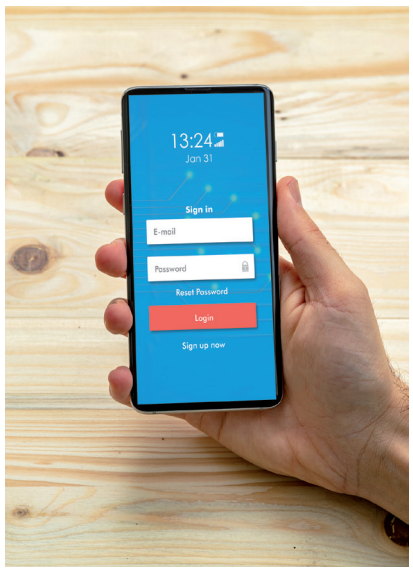
scrupuleusement respectées. N'oublions pas que les cybercriminels sont en mesure d'exploiter la moindre faille.

> Quel est leur mode opératoire ?

Pour parvenir à leurs fins, les pirates informatiques emploient des méthodes brutales, susceptibles d'impacter lourdement le fonctionnement d'un établissement de santé. Nous considérons deux cas concrets : une intrusion externe et une attaque par « rançongiciel » – également connue sous les noms de « cryptolocker » ou de « ransomware ».

> Comment procèdent-ils ?

La plupart du temps, un cybercriminel envoie un courriel contenant une fausse facture à un salarié d'un établissement de santé. Non sensibilisé, il clique sur la pièce jointe et l'autorise à exécuter le code malveillant qu'elle contient. Le virus se propage ensuite via le réseau interne, grâce à des vulnérabilités qui n'ont pas été corrigées ou à des mots de passe insuffisamment protégés. Le logiciel corrompu commence à chiffrer les données sur les serveurs et les postes de travail auxquels il peut avoir accès. Sur l'ordinateur du salarié, une demande de rançon s'affiche.



> Les cabinets de radiologie sont-ils exposés ?

Ils sont davantage visés par des intrusions externes. Cas d'école : un cabinet de radiologie souhaite installer un serveur d'imagerie médicale pour fournir un accès distant aux données de radiographie et d'IRM à ses professionnels de santé. Il fait alors appel à un prestataire qui n'est pas nécessairement formé à la sécurité informatique. Le serveur d'imagerie est configuré rapidement, sans limitation d'accès par un identifiant et un mot de passe. En utilisant un moteur de recherche spécialisé, un pirate informatique scanne Internet à la recherche d'un système vulnérable. Lorsqu'il le repère, il utilise des logiciels pour extraire toutes les informations qui s'y trouvent (images médicales, données administratives des patients…). Une fois aspirées, ces données sont mises à prix sur des sites clandestins.

> Quelles conclusions en tirez-vous ?

Ces deux exemples démontrent que le risque provient d'une suite d'erreurs évitables, qui auraient pu être rectifiées en amont, grâce à une « hygiène informatique » simple et adéquate.

> C'est-à-dire ?

Le chiffrement des sauvegardes, l'application systématique des mises à jour et le niveau de sécurité des mots de passe sont des paramètres déterminants. Certaines mesures préventives permettent assez facilement de réduire le risque, sinon de circonscrire rapidement les dommages subis.

> les données anonymisées restent des données de santé à caractère personnel

> Quelles sont les bonnes pratiques à respecter ?

Tout commence par le choix d'un prestataire compétent. Il convient notamment de s'adresser à un opérateur qualifié et formé à la sécurité informatique. Les contrats doivent comporter des clauses encadrant la gestion des données personnelles et les obligations de sécurité du prestataire. La formation et la sensibilisation des utilisateurs sont des enjeux tout aussi stratégiques, au même titre que la gestion des habilitations. L'accès aux données du patient doit répondre à un véritable besoin, justifié sur le plan médical. Il doit également être limité aux professionnels de santé participant à sa prise en charge.

> Quelle est la conduite à tenir en cas de crise ?

Certaines procédures contribuent à préserver la continuité de l'activité. C'est d'ailleurs un prérequis indispensable dans le domaine de la santé, où le bien-être des patients peut dépendre de la disponibilité d'un service. Plusieurs mesures peuvent être prévues en amont, telles que la sauvegarde régulière des données et leur conservation sur un équipement distinct, idéalement déconnecté. Si une violation de données personnelles a été constatée, les procédures de gestion de crise doivent inclure une notification automatique à la CNIL. Si le risque est élevé, les personnes concernées devront également être informées de la fuite.

> Quid de la surveillance ?

La surveillance est un point fondamental, ne serait-ce que pour prévenir d'éventuels incidents. Une veille efficace permet aussi de se tenir informé des failles existantes et des mesures nécessaires pour y remédier. Plusieurs organismes officiels ont déployé des services parfaitement adaptés à ces exigences.

> Lesquels ?

L'ANS[3] a développé « un portail d'accompagnement cybersécurité des structures de santé » (https://www.cyberveille-sante.gouv.fr). Outre des informations détaillées, elle apporte notamment une aide précieuse pour le signalement, la gestion et le suivi des incidents. De son côté, l'ANSSI[4] tient à jour différents documents de veille, d'alerte et de réponse aux attaques informatiques. Elle publie également des guides et des bonnes pratiques de sécurité, ainsi que des informations concernant différentes menaces. Sur son site Internet, la DGOS[5] met un mémento de sécurité à la disposition des établissements de santé (https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/article/memento-rgpd).

Les cybercriminels sont en mesure d'exploiter la moindre faille

> Quel appui la CNIL peut-elle apporter aux structures de santé ?

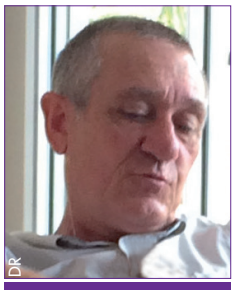
La CNIL propose différents outils en ligne pour accompagner tous les acteurs de santé dans leur démarche de mise en conformité. Les principaux intéressés pourront notamment se procurer un guide de la sécurité des données personnelles, mais aussi des logiciels et des guides pratiques qui facilitent la conduite et la formalisation d'analyses d'impact relatives à la protection des données, y compris pour les objets connectés.

Propos recueillis par Jonathan ICART

3. Agence du numérique en santé
4. Agence nationale de la sécurité des systèmes d'information
5. Direction générale de l'offre de soins

Dr Thierry BAUDOT, radiologue, médecin nucléaire – Nouméa

La radiologie dans la France des Outre-mers



Dr Thierry BAUDOT, médecin radiologue

Chaque territoire ultra marin est différent, majoritairement en zone tropicale. Pour simplifier, l'article s'appuie sur une vision personnelle de la situation radiologique à la Réunion (DOM[1]) et en Nouvelle-Calédonie (POM[2]).

> Pourquoi y exercer ?

Sur un plan personnel

- S'ouvrir à d'autres cultures et pouvoir explorer des parties du monde peu accessibles depuis l'Europe. Bémol, pour durer seuls les adaptables survivent, comme disent nos cousins du Québec : « Fait pas ton Français ! »
- Les sportifs trouveront un terrain de jeu exceptionnel… avec des températures clémentes toute l'année.
- Offrir à ses enfants une solide éducation, tournée vers le monde.

Sur un plan professionnel

Une démographie médicale plus favorable associée à un échantillonnage pathologique plus riche ouvre à une pratique d'excellence bien plus vite qu'en métropole.
C'est pour les jeunes radiologues finissants un tremplin exceptionnel. Bémol, il faut aimer les grosses charges de travail et la sur-spécialisation est souvent un frein.

> Vous en rêvez. Quelles sont les problématiques locales d'association ou de remplacement ?

Dans les DOM, pas de différence fondamentale avec un autre département. Dans les POM, c'est différent. Le droit d'exercice est conditionné à un conventionnement octroyé par le gouvernement local. Soit un collègue sur le départ vous cède son activité, soit vous prenez votre place dans une liste d'attente longue comme un bras en espérant qu'un jour les autorités ouvriront de nouveaux postes. Pour les remplacements, du côté des installés, la période est dure pour tout le monde…
Mais au final, le bouche à oreille vantant la qualité de la paye et le caractère très formateur font qu'il est assez facile de trouver d'excellents jeunes.

> Y a-t-il des difficultés de recrutement des personnels ?

Si c'est encore imaginable, les structures hospitalières publiques sont encore plus sous tension dans les Outre-mers que dans la mère Patrie… il n'est donc pas si difficile de recruter d'excellents manipulateurs (trices) d'abord attirés par une vision idyllique sous les cocotiers puis finalement assez heureux de pouvoir continuer leur rêve dans le privé.

> D'ailleurs quelles sont les relations avec le secteur public ?

Ni meilleures ni pires qu'ailleurs… tout est toujours une affaire de personnes.
De même en est-il avec les ARS[3] dans les DOM, la DDASS[4] et le gouvernement dans les POM.

> Et l'imagerie lourde avec autorisation préalable ?

Elle est bien présente, quoi que sans doute un peu plus rare qu'en Europe. Dans les DOM, la problématique d'autorisation est la même qu'à Lille ou Paris. Dans les POM, le système de santé est autonome et indépendant et l'autorisation passe par la DASS et le gouvernement local. Quel que soit le cas de figure, il est possible de s'équiper, mais comme partout, connaître les bons interlocuteurs politiques aide…

> Les questions qui fâchent, ou pourquoi s'en revenir… amer ?

En premier lieu, le coût de la vie. Les indicateurs officiels ont beau dire, lorsque, avec mon Caddy, j'effectue mes petites courses hebdomadaires dans la même enseigne qui optimise, je paie 35% de plus à la Réunion et 100% de plus à Nouméa par rapport à Saint-Jean-de-Luz !
Le marché de l'immobilier est aussi cher qu'à Paris.
Les choix culturels, alimentaires, vestimentaires… nécessitent de s'adapter ! Les rémunérations, on gagne plus… en dépensant plus et en travaillant… bien plus!

Sur le plan professionnel

Les marchés étant plus petits, le choix des matériels est plus réduit… et ils sont plus chers. ET LE GROS POINT NOIR… LE SAV. Il faut bien choisir ses partenaires car plus on s'éloigne des métropoles et plus les pannes durent longtemps… et plus les réparations sont onéreuses !

Pour conclure

S'installer dans les DOM TOM POM, c'est d'abord effectuer des remplacements accompagnés de ses proches afin de juger sereinement si un projet de bonheur familial peut s'envisager. C'est un paradis pour les sportifs, seul ou en famille… si vous aimez beaucoup travailler pour mériter votre temps libre. C'est une chance extraordinaire pour devenir des citoyens du monde, mais oublier son esprit français est un préalable pour durer. Plus on s'éloigne et plus les problèmes matériels demandent du recul, de la débrouille et un optimisme sans faille.

1. Département d'Outre-mer. 2. Pays d'Outre-mer. 3. Agence régionale de santé. 4. Direction départementale des affaires sanitaires et sociales

Florent LARUE, Interne en médecine générale

L'intérêt d'un passage en imagerie médicale dans le cadre de la formation de médecine générale

DR

Florent LARUE, interne en médecine générale

Je m'appelle Florent Larue, je suis interne en 5e semestre de médecine générale à la faculté de Montpellier. Un des stages de notre cursus, généralement effectué en fin d'internat, nous offre la possibilité d'effectuer des consultations en autonomie chez un praticien de médecine générale tout en assistant un à deux jours par semaine à des consultations d'autres spécialistes. Selon les intérêts de chacun, il nous revient donc de trouver un spécialiste acceptant de nous recevoir une demi-journée par semaine pendant trois à six mois.

Cette demi-journée consiste généralement à observer l'activité du praticien en question mais permet aussi parfois de l'assister dans sa pratique. Que ce soit en termes d'apprentissage pratique ou de gestes techniques, ce sont toujours des moments privilégiés et riche d'enseignements qui nous permettent d'avoir une idée bien plus précise de la pratique dans ces autres spécialités.

Si les choix des internes en médecine générale se portent le plus souvent sur des spécialités comme la dermatologie, la rhumatologie, la gynécologie ou encore la cardiologie, l'imagerie médicale n'est que très rarement plébiscitée.

Avant de commencer mon stage chez le Dr Béatrice Lognos Folco, médecin généraliste, je lui avais fait part de mon attrait pour l'imagerie qui n'était pas très répandu au sein de la promotion. Je m'aventurais donc en terrain inconnu en demandant, sur ses conseils, au Dr Patrick Souteyrand et ses associés s'ils accepteraient de me recevoir à la clinique du Parc de Castelnau-le-Lez (34) dans le service de radiologie a raison d'une demi-journée par semaine.

> Le choix de cette spécialité, qui en a surpris plus d'un parmi mes collègues, s'est révélé être l'un des plus formateur de mon semestre.

En effet, il n'est pas un jour en médecine générale ou l'on ne soit amené à demander un examen d'imagerie. Que ce soit échos, radios, IRM, TDM voire arthroTDM, nous sommes amenés à devoir jongler avec toutes ces modalités d'imagerie, parfois invasives pour le patient ou coûteuses pour le système de santé.

Il est de notre responsabilité d'orienter au mieux le patient pour qu'il puisse bénéficier de l'examen le plus approprié à sa symptomatologie en fonction de nos hypothèses diagnostiques et ceci afin d'éviter la multiplication des examens inutiles.

Néanmoins, nous avons peu l'occasion d'être en contact avec des radiologues et parfois tendance à délaisser cette spécialité ce qui fait que nos connaissances en imagerie remontent souvent à l'ECN[1].

Il ne m'a pas fallu longtemps pour constater le nombre d'examens d'imagerie prescrit[2] de façons inappropriées ou d'ordonnances manquant d'informations essentielles pour permettre au radiologue d'effectuer son travail de façon optimale.

Ce stage m'a permis de clarifier beaucoup de choses dans ma conduite à tenir pour de nombreuses pathologies en ce qui concerne le recours à l'imagerie. Cela m'a notamment amené à avoir une idée plus claire de l'examen le plus adapté en fonction de la pathologie recherchée.

De façon plus générale, en permettant un transfert horizontal des connaissances, généraliser ce genre de stages pourrait s'avérer très enrichissant. Cela permettrait de renforcer les relations et la compréhension mutuelle entre ces deux spécialités. Optimiser la coopération médecin généraliste/radiologue, c'est au final optimiser l'efficience dans le parcours de soin de nos patients, tout en nous permettant de mieux comprendre les subtilités de cette belle spécialité et éviter les écueils des demandes inappropriées.

1. Epreuves classantes nationales
2. Les médecins radiologues ne sont pas prescrits. Ils sont responsables du choix de l'examen pratiqué avec le médecin demandeur (Ndrl)

Disparition du Dr Gérard CALMET


DR

Gérard était un ami très cher, un associé hors pair, un radiologue et un syndicaliste engagé, il était un visionnaire, un guide.

De formation lilloise, il s'installa à Reims en 1980. Son ouverture, son enthousiasme, et sa pugnacité firent de lui un véritable leader apprécié de tous.

Très vite, il comprit que le métier de radiologue était un métier de collaboration pluridisciplinaire, ou le radiologue devait s'imposer comme médecin à part entière.

La communication était indispensable à ses yeux pour faire connaître notre métier, ce qui l'orienta tout naturellement vers le syndicalisme.

Il fut membre actif et reconnu de la FNMR départemental de la Marne et à l'échelon national en tant qu'administrateur et membre du bureau de la FNMR.

Il aimait écouter, échanger, s'enthousiasmer, lancer des projets et les défendre était une de ses passions. Il avait souvent un coup d'avance.

Son cabinet rémois de Saint-Remi était sa deuxième famille, sa création fut un des premiers établissements multidisciplinaire libéral de France et il sut très rapidement attirer de nombreux associés, ayant bien compris que le développement de la radiologie passait par le regroupement.

Il fut un promoteur engagé dans la sénologie et le dépistage organisé, il y engagea le département de la Marne, qui fut parmi les cinq premiers départements engagés sur le plan national, ce qui n'était pas une évidence ! Nous l'en remercions.

Il fut un très grand promoteur de la qualité, qui pour lui était, à l'instar des biologistes, un des meilleurs garants de la défense de notre profession et nous lui devons Labelix.

La liste est encore longue, ...

Tout son art, il l'a partagé avec passion et respect de tous les gens qu'il croisait, sa patientèle, ses collaborateurs, tous les membres de la FNMR.

Nous pensons tout particulièrement à toute sa famille, Kitou son épouse, ses trois filles Emmanuelle, Valérie, Sandrine, leurs conjoints et leurs enfants et leur présentons toutes nos condoléances.

Dr Jean-Louis JABINET
Trésorier FNMR de la Marne

Notre ami Gérard Calmet nous a quittés.
Gérard, à travers ses fonctions nationales de trésorier adjoint et de vice-président a été l'aiguillon de notre Fédération en matière de communication et surtout du lancement de la réflexion axée sur la qualité en radiologie. Gérard a été la cheville ouvrière de la création de Labelix. Sa minutie et son engagement au service de notre spécialité ont été d'une aide précieuse pour la reconnaissance de la radiologie libérale et sa représentation par la FNMR.
Le bureau de la FNMR présente ses sincères condoléances à Marie Christine et ses enfants.

Dr Jean-Philippe MASSON,
Président de la FNMR

Dr Roger ANTONNY
Nous venons d'apprendre le décès le 16 avril 2020 du Dr Roger ANTONNY, médecin radiologue à Laxou (54).
À sa famille et à ses proches, nous adressons nos confraternelles condoléances.

Dr Jean BENNET
Nous venons d'apprendre le décès le 10 février 2020 du Dr Jean BENNET, à l'âge de 96 ans. Il était médecin radiologue à Paris. À sa famille et à ses proches, nous adressons nos confraternelles condoléances.

Dr Roger BESSON
Nous venons d'apprendre le décès le 7 avril 2020 du Dr Roger BESSON, médecin radiologue à Paris.
À sa famille et à ses proches, nous adressons nos confraternelles condoléances.

Le nouveau bureau restreint de la FNMR

– Juin 2020 –

Président : **Jean-Philippe MASSON**

Premier Vice-Président
Bruno SILBERMAN

Secrétaires généraux
Jean-Christophe DELESALLE,
Jean-Charles LECLERC

Secrétaires généraux adjoints
Paul Marie BLAYAC,
Philippe COQUEL

Trésorier **Dominique MASSEYS**

Trésorier adjoint
Jean-Charles GUILBEAU

Vice-Présidents chargés de mission
Eric CHAVIGNY,
Eric GUILLEMOT,
Grégory LENCZNER

Vice-Présidents chargés des relations auprès des syndicats médicaux
Philippe ARRAMON TUCCO (CSMF),
Eric CHEVALLIER (Avenir spé),
Jean-Louis PUECH (SML),
Pierre-Jean TERNAMIAN (FMF)

Vice-Présidents
Jean-Charles BOURRAS,
François BRUNETTI,
Philippe CAQUELIN,
François CHAVATTE,
Alexandra COUPTEAU,
Alain FRANCOIS,
Sébastien THIRIAT

FMF **Élection FMF**

La FNMR félicite le Dr Corinne LE SAUDER pour son élection à la présidence de la Fédération des Médecins de France

Le Dr Corinne LE SAUDER, médecin généraliste et médecin ostéopathe, a été élue en remplacement du Dr Jean-Paul HAMON.

Le bureau de la FMF se compose désormais de :

- **Dr Mickael FRUGIER,** médecin généraliste à Le Vigen, vice-président représentant les généralistes ;
- **Dr Pierre-Jean TERNAMIAN,** médecin radiologue VP de la FNMR et **Dr Jean-Pierre FUSARI,** chirurgien maxillo-facial, vice-présidents, représentants des spécialistes et des médecins des plateaux techniques lourds ;
- **Dr Éric BLONDET,** neurochirurgien, **Drs Jean-Marc LARUELLE,** médecin généraliste et **Christophe THIBAULT,** médecin généraliste, secrétaires généraux ;
- **Dr Dominique DREUX,** médecin généraliste, trésorier ;
- **Dr Claire CADIX,** médecin généraliste, trésorier adjoint.

GARD

Le Syndicat départemental du Gard
a procédé au renouvellement de son Bureau
le 26 mars 2020

Président : **Dr Pierre de BRUNANCHON** (Nîmes)
Secrétaire général : **Dr Julien LACROIX** (Nîmes)
Trésorier : **Dr Céline BALZAN** (Nîmes)

HAUTE-GARONNE

Le Syndicat départemental de la Haute-Garonne
a procédé au renouvellement de son Bureau
le 27 février 2020

Président : **Dr Jean-Louis PUECH** (Toulouse)
Secrétaire général : **Dr Eric BRUGUIERE** (Toulouse)
Secrétaire adjoint : **Dr François de MAUPEOU** (Toulouse)
Trésorier : **Dr Frédéric BENOIT** (Blagnac)

MANCHE

Le Syndicat départemental de la Manche
a procédé au renouvellement de son Bureau
le 2 mars 2020

Président : **Dr Julien WERTHEIMER** (Coutances)
Secrétaire général : **Dr Aliou DIA** (Saint-Martin-des-Champs)
Trésorier : **Dr Olivier GONTRAN** (Granville)

PYRÉNÉES ORIENTALES

Le Syndicat départemental des Pyrénées Orientales
a procédé au renouvellement de son Bureau
le 10 mars 2020

Président : **Dr Alvian LESNIK** (Cabestany)
Vice-Président : **Dr Paul Marie BLAYAC** (Perpignan)
Dr Pierre PAYROT (Cabestany)
Secrétaire général : **Dr Pierre MAQUIN** (Perpignan)
Trésorier : **Dr Marc BRIHAT** (Perpignan)

OCCITANIE

L'Union Régionale des Médecins Radiologues de l'Occitanie
a procédé à l'élection de ses administrateurs auprès de la FNMR le 23 mai 2020

Titulaires :
Dr Frédéric BENOIT (31)
Dr Paul-Marie BLAYAC (66)
Dr Eric BRUGUIERE (31)
Dr Pierre DE BRUNANCHON (30)
Dr Katia GIOBBINI (11)
Dr François KLEIN (34)
Dr Daniel LAGARD (82)
Dr Alvian LESNIK (66)
Dr Sophie MENJOT DE CHAMPLEUR (34)
Dr Jean-Louis PUECH (31)

Suppléants :
Dr Jean-Philippe ALUNNI (82)
Dr Jérôme BENIS (34)
Dr Thierry BLANC (34)
Dr Marc BRIHAT (66)
Dr Gilles CADEL (31)
Dr Thomas LEMETTRE (81)
Dr Pierre MAQUIN (66)
Dr Patrick SOUTEYRAND (34)

10921 **14** Hérouville-Saint-Clair, **CHERCHE SUCCESSEUR**, cabinet 3 radiologues, 2 km du CHU de Caen. Regroupement avec 33 autres radiologues de Caen prévu en 2021-2022. Contact : Dr Mircea Ion Oarda : miroarda@gmail.com, Tél. : 06 07 51 17 57

10922 **30** Bagnols sur Ceze – SELARL 6 associés. Cause retraite **CHERCHE SUCCESSEUR**. 2 sites + TDM et IRM. Activité polyvalente, mammo, tomosynth. Pas de garde. Contact : Dr V. Segal – valerie.segal@orange.fr – 06 70 19 34 64

10923 **38** Proche de Grenoble **CHERCHE COLLABORATEUR OU ASSOCIÉ** en vue de cessation progressive d'activité et cession du cabinet. Activité : radio géné, écho, mammo, dentaire (Cone Beam). Accès IRM. Idéal pour 2 radiologues. Contact : dr-chabert@wanadoo.fr

10924 **56** Ploermel, région Bretagne, **CHERCHE REMPLAÇANT(E) ET/OU FUTUR ASSOCIÉ(E)**. Activité polyvalente : radio conv, écho sauf obsté, doppler, mammo souhaitée mais non obligatoire, accès TDM, IRM. Pas de garde. Pas d'astreinte. Contact : philippe.dalifard@orange.fr

10925 **57** Proche frontière Luxembourg, 1h30 de Paris par TGV, cède **CAUSE RETRAITE** cabinet dans maison médicale où exercent actuellement deux praticiens à mi-temps. Matériel et locaux récents. Très bonne activité. Contact : cimnorlor@orange.fr

10926 **57** SELARL 2 radiologues, cabinet de ville, **CHERCHE ASSOCIÉ(E)**. Activité : radio conv, écho, mammo, IRM et scan en GIE. Contact : imagerie.moselle@gmail.com

- **Vous pouvez consulter les annonces sur le site internet de la FNMR : www.fnmr.org**
- **Les adhérents de la Fédération peuvent déposer leur annonce directement sur le site à partir de l'espace adhérent**

MACSF

ÉPARGNE ET RETRAITE

FISCALITÉ
attractive

FLEXIBILITÉ
de sortie de son épargne

PLAN D'ÉPARGNE RETRAITE *Nouveaux horizons* POUR VOTRE RETRAITE

SOLUTIONS ÉVOLUTIVES
qui s'adaptent selon l'âge

STRATÉGIE
personnalisée

NOUVEAU RES RETRAITE(1) **:** découvrez les opportunités offertes par le plan d'épargne retraite de la MACSF.

Nos conseillers vous aident à **construire ou à optimiser** votre épargne retraite avec **des solutions sur mesure** qui correspondent à votre situation et vos besoins.

Mon rendez-vous Retraite : macsf.fr 3233 Service gratuit + prix appel

20_165 - 03/2020 - Crédit photo : Getty Images - Création : DPS LES INDÉS

PUBLICITÉ

(1) RES Retraite est un plan d'épargne retraite sous forme de contrat d'assurance vie de groupe à adhésion facultative individuelle, libellé en euros et en unités de compte, souscrit par l'ANPREPS (Association Nationale Pour la Retraite des Professions de Santé), auprès de la MACSF épargne retraite.
L'assureur ne s'engage que sur le nombre d'unités de compte et non sur leur valeur. Les montants investis sur les supports en unités de compte ne sont pas garantis mais sont sujets à des fluctuations à la hausse ou à la baisse dépendant en particulier de l'évolution des marchés financiers. La description et le fonctionnement des supports en unités de compte sont détaillés dans la notice d'information du contrat, dans les Documents d'Information Clés (DIC) et dans les Documents d'Information Clés pour l'Investisseur (DICI) ou dans les documents équivalents agréés par l'AMF, disponibles sur la page Supports financiers du site macsf.fr.
MACSF épargne retraite - Société Anonyme d'Assurances sur la Vie régie par le Code des assurances, au capital social de 58 737 408 €, entièrement libéré - Enregistrée au RCS de Nanterre sous le n° 403 071 095. MACSF assurances - SIREN n° 775 665 631 - Société d'Assurances Mutuelle - Entreprise régie par le Code des assurances - Sièges sociaux : cours du Triangle - 10 rue de Valmy - 92800 PUTEAUX - Adresse postale : 10 cours du Triangle de l'Arche - TSA 60300 92919 LA DEFENSE CEDEX/France.