Cybersécurité : comment les établissements publics peuvent-ils se protéger contre les cyberattaques ?

L'EXPERTISE WEKA

WEKA .media .jobs .fr

Sommaire

LE MOT DE L'ÉDITEUR

L'ampleur croissante du risque informatique pour les établissements publics, notamment les collectivités territoriales et les hôpitaux, suscite inquiétudes et questions au regard des toujours plus nombreuses cyberattaques recensées chaque année.

Mais ces dernières ne représentent cependant qu'un aspect de la cybersécurité et de la résilience des structures et services. Il faut davantage parler de sécurisation numérique avec, au cœur des enjeux, la protection des données. Loin d'être purement technique, ce sujet majeur doit faire partie intégrante de la stratégie de toute organisation. Les failles étant bien souvent humaines, l'acculturation aux outils numériques doit s'accompagner d'une sensibilisation de l'ensemble des acteurs publics pour un usage responsable et sécurisé.

Il est donc plus que jamais nécessaire d'informer et de former agents, managers, élus, aux risques encourus en cas de cyberattaques : dysfonctionnement des services publics locaux, perte de données, conséquences humaines et financières...

Retrouvez dans ce Livre Blanc des analyses et témoignages de spécialistes de la sécurité des systèmes d'information et de la protection des données personnelles, avec un focus sur la cybersécurité dans le milieu hospitalier, pour permettre à chacun d'appréhender au mieux ce sujet essentiel du 21e siècle.

Julien Prévotaux

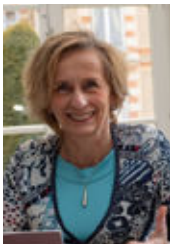
Directeur éditorial & des rédactions – WEKA

Cyberattaques : prévenir puis guérir

LES 10' JURIDIQUES

WEKA et le cabinet Landot et associés vous donnent rendez-vous toutes les semaines sur WEKA TV pour analyser l'essentiel de l'actualité juridique du monde territorial : l'expertise en 10 minutes au plus proche de vos besoins.

Eric Landot



Christine Bertrand

Éric Landot : Les cyberattaques, les rançongiciels et autres touchent désormais fréquemment les personnes publiques. La loi n° 2018-898 du 23 octobre 2018 relative à la lutte contre la fraude, l'avis de la commission supérieure du numérique n° 2021-03 du 29 avril 2021 portant recommandations dans le domaine de la sécurité numérique et de nombreux guides à retrouver sur cybermalveillance.gouv.fr le prouvent.

Sur ce même site, vous trouverez des exemples de calendrier de plans d'action et des infographies expliquant notamment les 5 clés pour une sensibilisation à la cybersécurité réussie. Vous pouvez également consulter le site de l'Agence nationale de la sécurité des systèmes informatiques (ANSSI), où se trouve le Guide d'hygiène informatique.

Il faut bien penser à avoir un suivi : externalisez votre suivi sur la cybersécurité pour avoir quelqu'un vers qui vous tourner. Dans ce domaine, il y a des labellisations qui sont sérieuses. En cas d'atteinte, consultez cybermalveillance.gouv.fr et faites en sorte d'éviter la contamination : débranchez ce qui doit l'être, mettez de côté vos backups, changez les adresses qui peuvent avoir été contaminées, etc.

Notre invité du jour, Mme Christine Bertrand, Directrice des systèmes d'information et numérique - Direction générale adjointe de l'administration et des ressources du Département de Seine-et-Marne, a accepté de répondre à nos questions.

Éric Landot : ***Comment bien réagir quand sa collectivité est victime d'une cyberattaque ?***

Christine Bertrand : La première des choses est de se poser la bonne question : il ne s'agit pas de se demander « est-ce qu'on sera attaqué ? » mais plutôt « quand ? ». Tout le monde peut potentiellement être attaqué. Il faut préparer en amont son plan de continuité et son plan de gestion de crise pour savoir quoi faire le jour où on sera attaqué.

Deuxième chose, il faut sécuriser son système d'information en privilégiant là aussi une sécurité avec des couches successives, avec des segmentations de zones, qui limitent les effets de l'attaque en empêchant la propagation. Ensuite, il faut sensibiliser les agents à tout ce qui est phishing et usurpation d'identité. La plupart des attaques commencent toujours par une usurpation d'identité d'un compte lambda. Enfin, il faut choisir sa sauvegarde en prévoyant une sauvegarde offline, à l'abri des attaques. La sauvegarde, c'est le dernier recours lors d'une cyberattaque.

Éric Landot : ***Quels sont vos conseils préventifs pour d'autres collectivités ?***

Christine Bertrand : Le premier conseil est de limiter la progression des impacts : débrancher le réseau est la première action réaliste. Deuxième chose, il faut informer en communiquant à différents niveaux : en interne, à la direction générale, vers vos partenaires, vers vos prestataires et surtout vers les citoyens. Il doit s'agir d'une communication adaptée en fonction de la cible et en fonction de l'attaque. L'objectif est d'éviter le blackout, garder le lien, garder la confiance et communiquer sur les enjeux et sur le plan de continuité d'activité.

Ensuite, il convient de porter plainte et d'informer la Commission nationale de l'informatique et des libertés (CNIL) pour tout ce qui concerne l'indisponibilité de services et la fuite de données.

Enfin, il vous faut investiguer sur l'attaque en elle-même en parallèle, pour vous permettre d'évaluer le périmètre, les dégâts et en déduire le plan de remédiation. En dernier lieu, vous devez réaliser ce plan de remédiation pour arriver à un rétablissement du service et, tout au long de ces étapes, toujours communiquer.

La plupart des attaques commencent toujours par une usurpation d'identité d'un compte lambda.

Les organisations publiques face au défi de la cybersécurité

PARLEZ VOUS PUBLIC

Échanges, analyses, débats : l'émission Parlez-vous public décrypte l'actualité de la fonction publique et de l'action publique locale. Parlez-vous public est une émission proposée par WEKA en partenariat avec la Casden Banque populaire, la banque coopérative de la fonction publique. Le principe de cette émission est simple : un thème, deux intervenants et trois questions. Voici un extrait de l'émission consacrée à la cybersécurité.

Hugues Périnel

Françoise Gatel

Général Marc Watin-Augouard

Hugues Périnel : L'ampleur du risque cyber pour les organisations publiques, notamment les collectivités territoriales et les hôpitaux, suscite de nombreuses inquiétudes et questions. Loin d'être purement technique, ce sujet majeur doit faire partie intégrante de la stratégie de toute organisation privée comme publique. Il est donc plus que jamais nécessaire d'alerter, de sensibiliser les élus et les fonctionnaires à l'existence de lourdes conséquences en cas de cyberattaques : dysfonctionnement des services publics, perte de données, conséquences humaines et financières… Nous avons souhaité contribuer à leur information sur les moyens de prévention en matière de sécurité et de résilience en cas d'attaque.

Pour le faire, nous avons deux invités pour en parler, que je m'empresse de présenter. Françoise Gatel est sénatrice d'Ille-et-Vilaine, présidente de la délégation sénatoriale aux collectivités territoriales et à la décentralisation, et auteure, parmi d'autres, d'un rapport d'information au Sénat avec Serge Babary, fait au nom de la délégation des entreprises et de la délégation aux collectivités territoriales, dont le titre est « Les collectivités territoriales face aux défis de la cybersécurité ». Le Général Marc Watin-Augouard est fondateur du FIC, le Forum international de la cybersécurité, président de l'Institut national pour la cybersécurité et la résilience des territoires et a dirigé pendant 9 ans le Centre de recherche de l'école des officiers de la gendarmerie nationale.

Ma première question porte sur le périmètre sur lequel la cybersécurité doit être appréhendée. Très souvent, on entend que telle collectivité, tel hôpital a subi une cyberattaque. Ne doit-on pas dépasser les organisations elles-mêmes pour réagir ? Peut-être au niveau intercommunal, peut-être au niveau régional, voire plus, et aussi peut-être dépasser la frontière entre le public et privé ?

Françoise Gatel : Merci pour l'invitation à cette émission sur un sujet dont le Sénat a voulu se saisir en lien avec la délégation aux entreprises puisque nous sommes intimement convaincus qu'il est nécessaire de sensibiliser les collectivités, quelles que soient leur taille, qui pensent que les cyberattaques concernent des structures de profits, donc des entreprises, et que ça ne peut pas leur arriver alors même que c'est arrivé dans les hôpitaux, même dans une station d'épuration, dans des petites collectivités, quelle que soit leur taille.

Nous avons remarqué l'augmentation du risque et des attaques ainsi que le peu de connaissances et l'insuffisante appréhension par tous les élus de ces sujets. Quand vous êtes une commune de 150 habitants, il est évident que vous n'avez ni le budget, ni les personnels qualifiés pour identifier le risque, se l'approprier et mettre en œuvre les moyens nécessaires. Donc vous avez parfaitement raison, il est absolument indispensable de travailler à une échelle de coopération qui soit efficace pour gagner du temps, avoir de l'expertise et des solutions.

Cela est d'autant plus important dans les collectivités car aujourd'hui nous avons des connexions des systèmes d'information. Souvent, à l'échelle d'une intercommunalité, vous avez un dispositif de système d'information qui est partagé par toutes les collectivités qui en sont membres, voire des syndicats. Cela signifie que le maillon faible peut être la voie d'entrée du hacker et affaiblit tout le monde. Il faut donc travailler à une échelle pertinente et je suis personnellement assez favorable à ce qu'il y ait aussi des liens entre des entreprises et des collectivités. Donc travaillons à une échelle qui va aider à contaminer positivement la prise de de conscience et qui, surtout, donnera des moyens humains et aidera à résoudre les choses par des échanges de bonnes pratiques.

Hugues Périnel : ***On voit bien l'importance du collaboratif et du coopératif. Au-delà de ce point, il y a aussi, à l'intérieur de ces organisations, une question posée au management en ce qui concerne la formation à des nouveaux métiers, des cybermétiers, qui n'existent pas dans ces petites structures.***

Général Marc Watin-Augouard : Vous avez raison, aujourd'hui, il faut vraiment travailler sur les territoires en coopération, en collaboration. Pourquoi ? Parce que toute l'histoire de notre cybersécurité en France est une histoire qui est partie du haut et qui est descendue vers le bas, mais au travers de silos très précis. C'est-à-dire que nous avons commencé à se poser la question sur les opérateurs d'importance vitale, ceux sur lesquels il faut absolument se reposer si on veut pouvoir continuer à vivre tous les jours. Les grands opérateurs sont l'énergie, l'information, la santé. Ce faisant, nous avons laissé de côté un certain nombre d'acteurs : les petites entreprises, les collectivités territoriales et les services publics locaux, en se disant finalement que ces derniers ne seront jamais atteints mais cela est faux. Il n'y a pas de périmètre : vous êtes connecté, vous serez une cible potentielle. Soit une cible directe, soit une cible indirecte.

Toutes nos données sont aujourd'hui dans les mains des collectivités territoriales.

Si on prend l'exemple d'un maire d'une commune de 1 500 habitants, comme la mienne, quand je lui parle de l'activité de sa commune et que nous faisons l'inventaire de toutes les données qui sont récoltées, c'est absolument phénoménal : le cadastre, les informations sociales, les informations concernant la cantine scolaire, la bibliothèque scolaire, la maison de santé, l'EHPAD… Toutes nos données sont aujourd'hui dans les

mains des collectivités territoriales, chacune, bien sûr, n'ayant que les données qui les concernent selon les compétences exercées. Mais cela vous montre bien qu'il y a une mine extraordinaire. Or, la donnée est de l'or noir. Il s'agit de la matière première, de la richesse du 21e siècle. Et cette donnée a une valeur, on peut soit l'échanger contre une rançon ou on peut l'utiliser pour l'exploiter et tirer des enseignements sur un territoire.

Aujourd'hui, on ne peut pas accepter d'abandonner les collectivités territoriales et donc pour moi, il faut, après la verticalité de l'action sur les opérateurs les plus essentiels, s'intéresser à l'horizontalité des territoires. Qu'est-ce qu'un bon territoire ? J'aurais tendance à dire que si l'on veut une action globale, c'est le département, mais pour les collectivités territoriales, je partage complètement votre analyse, il faut passer au niveau des établissements publics de coopération intercommunale (communauté d'agglomération, métropole, etc.). Mais nous ne pouvons plus laisser les petites communes en déshérence. Pourquoi ? Parce qu'un jour elles seront, sinon visées directement, visées comme point de départ. C'est à dire qu'on l'attaquera pour faire un saut de puce et attaquer la commune plus importante et ainsi de suite.

Notre **défaillance** est liée au fait que nous ne sommes pas suffisamment **acculturés aux enjeux du cyber.**

Donc aujourd'hui, c'est un véritable enjeu et vous l'avez dit vous-même, il faut d'abord former les élus. Ensuite, il faut former des personnes en mesure d'apporter une aide aux collectivités territoriales. Avec une l'association pour l'enseignement numérique, nous avons créé, il y a peu de temps aux Sables d'Olonne, la première formation pour les RSSI, responsables de la sécurité des systèmes d'information des collectivités territoriales. Ce sont des jeunes à qui on va apprendre ce qu'est une collectivité territoriale, comment elle fonctionne et comment on peut la protéger.

Bien sûr, la petite commune ne pourra pas se le payer, mais une communauté d'agglomération, elle, pourra peut-être s'en payer un à temps partiel, puis la métropole et puis le département peut-être. Et ainsi, nous allons fédérer, faire en sorte que personne ne soit abandonné.

Hugues Périnel : ***Avons-nous vraiment conscience de la place que représente le facteur humain ? Car le facteur humain peut permettre de démultiplier ou de réduire les risques.***

Général Marc Watin-Augouard : L'Agence nationale pour la sécurité des systèmes d'informations le dit : 85 % des problèmes qui existent sur notre espace numérique sont liés à notre propre défaillance. Et notre défaillance est liée au fait que nous ne connaissons pas, nous ne sommes pas suffisamment acculturés aux enjeux du cyber. Si déjà on forme les personnels, si on forme la secrétaire ou le secrétaire de mairie, si on forme les agents des services publics locaux en leur disant « attention, il y a un enjeu » ou « attention, il y a des actes d'hygiène informatique ». Quand vous rentrez chez vous, vous ouvrez la porte, mais quand vous sortez, vous la fermez. Si vous ne faites pas ces actes essentiels dans le monde numérique, les mêmes que vous accomplissez dans le monde réel, alors il ne faut pas s'étonner d'être cyber attaqué.

Retrouvez l'intégralité de votre émission Parlez-vous-public sur la WEKA TV : https://www.weka.fr/actualite/weka-tv/parlez-vous-public/les-organisations-publiques-face-au-defi-de-la-cybersecurite-150772/

Cybersécurité : une méthode clé en main pour sensibiliser les agents des collectivités

L'AMF s'est associée à Cybermalveillance.gouv.fr pour éditer un guide méthodologique destiné à sensibiliser les agents des collectivités à la cybersécurité.

À l'occasion du 104e Congrès des maires et des présidents d'intercommunalités de France, Cybermalveillance.gouv.fr, dispositif national d'assistance aux victimes d'actes de cybermalveillance, et l'AMF ont dévoilé, le 18 novembre 2022, une méthode « clé en main » destinée à sensibiliser les agents des collectivités aux enjeux de la cybersécurité. Ce guide méthodologique de 16 pages s'adresse à toutes les collectivités territoriales, sans exception, très exposées et néanmoins peu conscientes du risque encouru. En effet, le risque cyber est omniprésent – Cybermalveillance.gouv.fr a enregistré une augmentation de près de 70 % de demande d'assistance en ligne en 2021 – et les collectivités ne peuvent pas y échapper.

Une étude réalisée au cours du second semestre 2021 par Cybermalveillance.gouv.fr auprès des collectivités de moins de 3 500 habitants a mis en exergue leur faible préparation aux cyberattaques. Au-delà d'un manque de connaissance et d'information sur le sujet pour plus des deux tiers des publics concernés (maires, adjoints, DGS et agents), l'étude a révélé le défaut de formation à la cybersécurité des responsables ou des prestataires informatiques des collectivités. Ces résultats prouvent que les collectivités territoriales constituent une cible particulièrement vulnérable.

Cybermalveillance.gouv.fr et l'AMF ont donc élaboré une méthode clé en main pour sensibiliser et responsabiliser tous les agents. « On le sait aujourd'hui, de nombreuses attaques ciblent l'humain. Un utilisateur averti permet de réduire considérablement les risques et contribue même à élever le niveau de sécurité collectif, d'où la nécessité d'impliquer toute la collectivité dans cette démarche, du stagiaire à l'élu en passant par les

agents », insistent les rédacteurs du guide. Fort de ces constats, Cybermalveillance.gouv.fr et l'AMF ont conçu un dispositif composé, à la fois, d'une approche théorique et d'un plan d'action facile à mettre en œuvre, accompagnés d'un ensemble d'outils et de contenus pédagogiques. Ainsi, la méthode clé en main s'adresse à l'ensemble des collectivités qui initient une démarche de sensibilisation. « Présentée dans son intégralité, elle est une illustration idéale d'un programme de sensibilisation global. Sa mise en œuvre dépendra de la priorité donnée au risque cyber, de la disponibilité et des ressources à y dédier », soutiennent ses concepteurs.

Cette méthodologie se veut une « boîte à outils cyber », modulable et personnalisable. Elle détaille « 5 clés pour une sensibilisation réussie ». Au programme :

- Clé n° 1 : Prendre conscience du risque cyber
- Clé n° 2 : Impliquer les publics des collectivités
- Clé n° 3 : S'appuyer sur les bonnes ressources pédagogiques
- Clé n° 4 : Décliner et répéter les messages
- Clé n° 5 : Vérifier l'assimilation des messages

Traduction pratique, le guide propose ensuite un exemple de programme de sensibilisation des agents, en trois actes.

« Les agents des collectivités constituent le premier maillon de la chaîne de sécurité face au risque cyber dans nos communes. Faire face aux crises, c'est s'y préparer et toutes les actions présentées dans ce guide sont autant de clés permettant d'augmenter l'immunité de nos collectivités », explique le président de l'AMF David Lisnard. « De nombreuses attaques pourraient être évitées avec une sensibilisation aux risques numériques efficace et un apprentissage des bonnes pratiques au quotidien. Au travers de cette méthode « clé en main » coéditée avec l'AMF, nous avons voulu doter les collectivités des clés nécessaires pour appréhender le sujet, préparer, former et responsabiliser les agents face aux enjeux de la cyber et en faire de véritables partenaires de la sécurité de leur collectivité », complète Jérôme Notin, directeur général du GIP ACYMA, la structure qui pilote le dispositif national Cybermalveillance.gouv.fr.

De nombreuses attaques pourraient être évitées avec une sensibilisation aux risques numériques efficace et un apprentissage des bonnes pratiques au quotidien.

FICHE MÉTHODOLOGIQUE WEKA

Fiche 11161

Désigner un délégué à la protection des données

1 outil associé

CONTEXTE

Avec l'entrée en vigueur du règlement général pour la protection des données (RGPD), les obligations de la collectivité à l'égard des traitements de données personnelles ont beaucoup changé.

S'il n'est plus (ou plus systématiquement) nécessaire de solliciter des autorisations ou de déposer des déclarations lors de la création d'un traitement de données personnelles, toute collectivité se doit désormais de mener une politique responsable et autonome de gestion de ses traitements. Pour ce faire, elle doit nommer une personne qui en est plus spécifiquement chargée : le délégué à la protection des données (DPD). Voici ce qu'il faut savoir pour le désigner.

Schéma
Désigner un délégué à la protection des données

Notre schéma vous indique la procédure à suivre pour nommer ou remplacer un délégué à la protection des données (DPD). Si la notification à la Cnil ne présente pas, en elle-même, de difficulté particulière, la réflexion autour du choix du DPD mérite quant à elle d'être accompagnée.

▶ 1 - Comprendre que la désignation du DPD est le plus souvent obligatoire, mais aménageable

Aux termes du RGPD, **la désignation d'un DPD est obligatoire** pour toutes les personnes publiques effectuant des traitements de données. Toutes les collectivités locales et tous les EPCI sont concernés, ainsi que les établissements publics administratifs et industriels et commerciaux.

Il s'agit d'une différence notable par rapport à la réglementation antérieure, qui prévoyait l'instauration facultative d'un correspondant informatique et libertés (CIL).

Par ailleurs, les communes peuvent se doter d'un **délégué à la protection des données commun**. Un seul DPD peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

A noter

À la lettre des textes, vous devez avoir nommé un délégué à la protection des données depuis le 25 mai 2018. Ne tardez pas, donc, si ce n'est pas encore fait.

▶ 2 - Comprendre l'étendue des missions du DPD

L'étendue des missions du délégué à la protection des données est très importante. Il joue à la fois un rôle de vigie, de sensibilisation, de détenteur de toute l'information relative aux données personnelles, et de garant de la conformité des traitements à la réglementation.

Ainsi, il sera de sa compétence :

- D'**informer le maire et les membres du conseil municipal, ainsi que les agents de la collectivité**, sur les obligations qui leur incombent en matière de traitement des données personnelles. Des rapports réguliers doivent ensuite permettre aux agents et aux décideurs de suivre les évolutions de la politique de protection des données de la collectivité.
- De **formuler par écrit ses avis et recommandations** à chaque fois qu'il sera sollicité. À cet égard, le RGPD précise que le DPD doit tenir dûment compte, dans l'accomplissement de ses missions, « *du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement* ».
- De **former ou à tout le moins de sensibiliser les agents** quant à leurs obligations, aux bonnes pratiques à respecter et aux engagements qu'ils devront, le cas échéant, exiger de leurs cocontractants.
- D'**auditer les risques** concernant les traitements de données et d'établir une cartographie des risques de non-conformité. Des mesures correctives, de suivi ou d'alerte doivent le cas échéant être mises en place.
- De **piloter la documentation** relative aux traitements de données, et notamment les études d'impact à réaliser lors de la mise en place d'un traitement.
- De **contrôler**, dans le cadre de sa mission d'audit, la bonne mise en œuvre des dispositifs mis en place, et le **respect des procédures de collecte et de traitement des données**.
- De **réaliser les formalités à accomplir lorsqu'une faille de sécurité** a été constatée.
- De servir de **point de contact avec la Commission nationale de l'informatique et des libertés** (Cnil) ou toute autorité nationale de protection des données.
- De **se tenir (formé et) informé de toutes les évolutions de la réglementation** qui pourraient avoir des conséquences sur la conformité des traitements de la collectivité.

A noter

La tenue du registre des traitements, qui est désormais un document obligatoire pour chaque collectivité, n'incombe pas forcément, à la lettre des textes, au délégué à la protection des données. Ce sont deux obligations distinctes. Mais en pratique, il est logique que le DPD prenne en charge la tenue de ce registre.

Les services de la collectivité devront également garder à l'esprit quel est son rôle, l'informer de tout projet de création d'un nouveau traitement de données et l'associer à cette création.

▶ 3 - Décider de recourir à un agent ou à un prestataire externe

Le RGPD et la loi informatique et libertés laissent à la collectivité le libre choix de la personne qui exercera la fonction de délégué à la protection des données. Il peut s'agir d'un agent de la collectivité ou d'un prestataire extérieur.

Le choix d'un agent interne à la collectivité : maîtrise, disponibilité, implication

Choisir comme délégué à la protection des données un agent de la collectivité présente un avantage indéniable : cet agent sera dédié aux seuls traitements de données de la collectivité. Il n'aura pas d'autres « clients », qui pourraient l'amener à négliger ses missions auprès de vous.

Pour autant, cet agent doit **détenir certaines qualifications indispensables**, encore peu répandues. Ainsi, si vous choisissez de nommer DPD un agent déjà présent au sein de la collectivité, il vous faudra assurer sa formation. Il ne sera donc pas opérationnel immédiatement. Si vous choisissez de recruter un agent, il faut savoir que **la demande est importante** et que le nombre de personnes compétentes, s'il ne fait que croître, est inférieur aux besoins. Le recrutement par concours pourra, à cet égard, s'avérer complexe.

Par ailleurs, il convient d'avoir présent à l'esprit que la faible disponibilité de personnes compétentes sur le marché fait que **ce type de mission se paie cher**. Actuellement, dans le secteur privé, les montants annuels de salaire jugés « honorables » s'étalent entre 35 000 €/an pour un DPO débutant et environ 100 000 €/an dans les très grosses structures, avec de fortes responsabilités. Il pourrait donc s'avérer difficile, pour une collectivité, d'être attractive pour recruter ce type d'agent à temps plein.

Enfin, sachez que l'agent désigné comme DPD ne pourra pas être rattaché à n'importe quel service de la collectivité. En effet, il **ne doit pas se trouver en situation de conflit**

d'intérêts. Par exemple, en tant que garant de la sécurité des traitements de données au sein de la collectivité, il n'est pas recommandé de le placer sous la responsabilité du responsable des services d'information. Celui-ci pourra en effet refuser certains aménagements proposés sans que le DPD ose s'y opposer, en tant que subordonné.

Le DPD ne peut pas davantage, dans l'idéal, être responsable RH ou responsable informatique, dans la mesure où, au titre de ces fonctions, il sera amené à gérer des fichiers de données personnels. **Il ne peut donc être à la fois « donneur d'ordres » et « contrôleur »**.

A noter

Si le délégué à la protection des données doit être une personne nommément désignée, vous pouvez, dans les faits, constituer une équipe chargée de la protection des données au sein de la collectivité.

Le choix d'un prestataire externe : rapidité, compétence, accompagnement

Recourir à un prestataire extérieur peut s'avérer à la fois moins coûteux et plus rapide que de devoir désigner et former un agent au sein de la collectivité. En effet, de nombreuses sociétés spécialisées sont d'ores et déjà opérationnelles pour accomplir ce type de missions. Elles proposent d'ailleurs souvent des prestations annexes, comme la mise à disposition d'un logiciel récapitulatif des traitements, permettant d'éditer un registre et de gérer les durées de conservation des données au cas par cas.

Par ailleurs, **nombre de vos conseils habituels peuvent s'avérer compétents** pour assumer la mission de DPD : avocat, commissaire aux comptes, expert-comptable. Ces nouvelles missions viendront bien entendu en surcharge, mais il est possible, à l'occasion du renouvellement des marchés concernés, de prévoir un lot spécifique sur ce point.

Dans ce cadre, il faudra évaluer le montant possible des prestations, et **lancer un marché public de services dans les formes requises** par le Code de la commande publique. Eu égard aux montants en jeu, et sauf si votre collectivité est très importante, le montant pourrait ne pas excéder le seuil de procédure adaptée de 90 000 € (si l'on exclut l'audit initial). Il faudra s'assurer de l'indépendance et de l'absence de conflits d'intérêts. Ainsi, vous ne pourrez confier le marché « DPD » à votre prestataire informatique habituel.

▶ 4 - Prévenir la Cnil de la nomination du DPD

La procédure de nomination du DPD est très simple, il suffit de **remplir le formulaire** disponible sur le site de la Cnil : www.cnil.fr/fr/designation-dpo.

Il s'agit d'une procédure très simple, qui ne devrait pas prendre plus de 5 à 10 minutes, sur le site de la Cnil, si votre connexion à Internet est correcte. Les informations qui vous seront demandées dans ce cadre sont très simples et directes, voici les quatre étapes pour finaliser la désignation :

1/ organisme ;

2/ délégué ;

3/ coordonnées publiques ;

4/ récapitulatif et envoi.

▶ 5 - Permettre un accès direct du public au DPD

Le délégué à la protection des données n'est pas seulement l'autorité de référence pour les agents de la collectivité, il doit être le **point de contact pour toute question** posée par une personne concernée par un traitement. Ainsi, il doit pouvoir être joint facilement, par téléphone, courrier ou courriel.

Des informations spécifiques le concernant peuvent être mentionnées sur le site Internet de la collectivité, expliquant ses fonctions et communiquant les coordonnées où le joindre. Le cas échéant, un formulaire de contact peut être intégré dans cette page.

NOTRE CONSEIL

Choisir un agent ou un prestataire extérieur ?

Ce choix va dépendre du nombre de traitements et de l'importance de votre collectivité. Y a-t-il matière à occuper un agent à temps plein ? Disposez-vous dans votre effectif d'un agent qui, moyennant une formation, pourrait assumer cette fonction ? Un prestataire extérieur coûterait-il nécessairement plus cher que de rémunérer un agent ?

En l'état du faible niveau de formation de la majorité des agents concernant le droit des données personnelles, la meilleure solution pourra être, plus d'une fois, de recourir à un prestataire extérieur qui formera un binôme avec l'agent pressenti pour devenir DPD. Ce prestataire pourra se charger du travail de diagnostic initial des traitements de la collectivité, et pourra ensuite s'effacer, en vitesse de croisière, pour n'apporter des conseils qu'en cas de question pointue ou épineuse.

Vérifier les qualifications de votre prestataire

N'est pas DPD qui veut. Une formation professionnelle solide est indispensable, et une assurance professionnelle compatible avec les fonctions de DPD est obligatoire. Il conviendra donc, dans le cadre de l'appel d'offres que vous lancerez, de vous assurer que les candidats en disposent. Par ailleurs, le cahier des charges devra être solidement construit.

ÉVITEZ LES ERREURS

N'ajoutez pas simplement une mission à l'un de vos agents

Il faut que vous soyez conscient que la mission de DPD peut s'avérer très chronophage. Ce n'est pas une mission qui peut être assumée « en plus » sur une fiche de poste inchangée. Ainsi, si vous choisissez un agent dans vos rangs pour assurer la mission de DPD, il faudra remettre à plat sa fiche de poste, et lui dégager du temps pour qu'il puisse assumer sérieusement ses nouvelles missions.

Ne pensez pas que ce nouvel agent sera forcément bien accueilli

Il n'est pas question ici d'opposition directe des agents à l'intervention du DPD, comme cela peut arriver dans le cadre d'audits réalisés sur certains services où l'on a constaté des dysfonctionnements. Il s'agira bien souvent d'attitudes plus insidieuses : les agents, n'ayant jusqu'à présent jamais eu besoin d'associer un référent « données personnelles » à leurs projets impliquant la création d'un traitement de données, ne verront pas nécessairement l'utilité d'associer cet agent au projet et à la prise de décision. Un travail de sensibilisation aux enjeux est ici indispensable. Il peut être fait par un formateur extérieur ou par des plaquettes d'information, qu'il convient de diffuser le plus largement possible.

Ne pensez pas qu'il suffit d'informer les chefs de service sur les fonctions du DPD

En effet, les responsables de services (RH, DSI, petite enfance) sont de prime abord les plus concernés, car ils gèrent des effectifs, des fichiers, ou encore des services à la population. Pour autant, n'importe quel agent est susceptible de créer un fichier contenant des données personnelles, sans penser à mal, et même sans imaginer que son fichier Excel est un traitement de données. Ce peut être le cas d'un agent de la reprographie qui notera les différentes commandes reçues et les noms de leurs destinataires, d'une personne chargée d'accueil qui de son propre chef enregistrera les visiteurs accueillis chaque jour ainsi que le motif de leur présence, etc.

FAQ

Puis-je conserver mon correspondant informatique et libertés après l'entrée en vigueur du RGPD, et me dispenser de nommer un DPD ?

Non, le statut de CIL a disparu le 25 mai 2018, avec l'entrée en vigueur du RGPD et la disparition des textes anciens. Désormais vous devez nécessairement désigner un délégué à la protection des données.

Le correspondant informatique et libertés désigné avant l'entrée en vigueur du RGPD devient-il automatiquement DPD ?

Non, cette désignation n'a aucun caractère automatique, même s'il peut être tentant, pour assurer la continuité, de faire confiance au même agent. Avant toute chose, il faut vérifier

que le CIL remplit les conditions de compétences nécessaires à sa désignation en tant que DPD, et le cas échéant le former.

Ensuite, il conviendra de mener la procédure de désignation du DPD auprès de la Cnil dans son intégralité. La désignation préalable d'un CIL n'offre aucune « avance », de ce point de vue.

Que faire si la collectivité n'arrive pas à recruter un DPD ?

Si vous souhaitez procéder à un recrutement extérieur, effectivement, le poste peut être compliqué à pourvoir. Dans ce cas de figure, conservez précieusement la trace de toutes les démarches effectuées pour parvenir à ce recrutement, pour montrer votre bonne volonté.

Posez-vous aussi les bonnes questions : ce poste ne peut-il pas être pourvu en interne, en chargeant un agent de cette tâche ? Puis-je externaliser la fonction (dans le cadre d'un marché public, par exemple), au moins pour la phase de diagnostic et de mise en conformité initiale ?

Existe-t-il des outils susceptibles d'aider le DPD dans ses tâches ?

Oui, des outils de plus en plus nombreux sont en cours d'élaboration par la Cnil pour assister le DPD dans ses missions, par exemple le logiciel *open source* PIA (*Privacy Impact Assessment*) qui permet de mesurer l'impact des traitements sur les données personnelles en facilitant la conduite et la formalisation d'analyses d'impact sur la protection des données telles que prévues par le RGPD. En termes plus clairs, ce logiciel permet d'aider le DPD à déterminer si ces traitements sont compatibles avec les règles du RGPD.

Par ailleurs, de nombreux logiciels de marché permettent de tenir le registre des traitements, et proposent un accompagnement semi-guidé pour les collectivités.

Quelle est l'étendue de l'obligation d'alerte du DPD ?

Le devoir d'alerte du DPD à l'égard du maire et du conseil municipal est certain, puisqu'il est le fondement même de la fonction : donner à la collectivité les moyens de diagnostiquer les non-conformités et de les corriger.

En revanche, et même si le RGPD est muet sur ce point, il ne semble pas tenable que le DPD doive dénoncer la collectivité ou ses décideurs en cas de non-conformité persistante. Il y aurait, s'il s'agit d'un agent, un manquement à son devoir de loyauté, et dans tous les cas une perte de confiance.

Le DPD se substitue-t-il à la Cnil pour contrôler les traitements de la collectivité ?

Non, la Cnil conserve l'intégralité de sa fonction de contrôle. Le délégué à la protection des données sera, dans ce cadre, son interlocuteur privilégié en cas de contrôle.

Comment mettre fin aux fonctions du DPD ?

Si la désignation du DPD doit être faite en respectant une procédure strictement définie, aucun texte ne prévoit pour le moment comment mettre fin à ses fonctions.

Si je change de DPD, dois-je de nouveau le notifier à la Cnil ?

Oui. Cette formalité a pour objet de communiquer au régulateur les coordonnées de celui qui sera son point d'entrée au sein de la collectivité. Il doit donc disposer d'un contact en fonction.

Quels rapports le DPD entretient-il avec les instances représentatives du personnel ?

Le DPD n'exerce, sur le fondement des textes, aucune fonction à l'égard des instances représentatives du personnel. Il se doit toutefois de répertorier les traitements de données existants, s'ils sont internes à la collectivité. Dans certains cas, il sera associé à l'information des représentants du personnel lorsqu'un traitement concerne les agents de la collectivité.

Le DPD peut-il être considéré comme un agent protégé ?

Une réponse ministérielle a indiqué (à propos d'un DPD salarié de droit privé) que le DPD

n'est pas un salarié protégé au sens du droit du travail, même s'il bénéficie d'une protection spécifique prévue par la législation sur les données personnelles (Rép. min. n° 02896 : *JO Sénat*, 7 févr. 2019). Il ne peut ainsi « *être relevé de ses fonctions ou pénalisé par le responsable de traitement ou le sous-traitant pour l'exercice de ses missions* » (RGPD, art. 38). Sont concernées les sanctions même indirectes telles que l'absence de promotion, les freins à l'avancement de carrière ou le refus d'octroi d'avantages dont bénéficient d'autres travailleurs. Cette position de l'administration est sans nul doute opposable aux DPD employés par une collectivité publique.

ALLER PLUS LOIN

Outil

Légende de schéma de procédure

Cette légende vous permet de suivre chaque étape des procédures décrites dans les schémas et d'en comprendre la nature.

Références juridiques

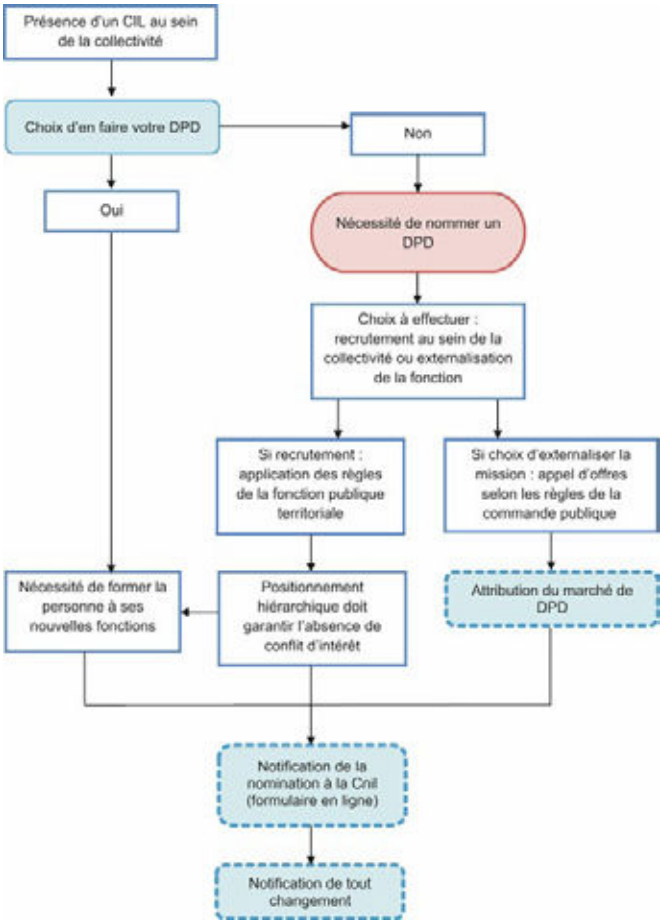
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Réponse ministérielle n° 02896 : *JO Sénat*, 7 février 2019

Site Internet

www.cnil.fr/professionnel : site de la Cnil, espace professionnel, où trouver :

- différents articles permettant au délégué à la protection des données de prendre ses fonctions ; rubriques Ma conformité au RGPD > Passer à l'action > Le délégué à la protection des données (DPO) > DPO : par où commencer ?
- le logiciel *open source* PIA, qui facilite la conduite et la formalisation d'analyses d'impact sur la protection des données telles que prévues par le RGPD ; rubriques Ma conformité au RGPD > Les outils de la conformité > L'analyse d'impact (AIPD) > Outil PIA
- le formulaire de nomination du DPD ; rubriques Ma conformité au RGPD > Services en ligne > Désigner un délégué (DPO)
- les lignes directrices sur le délégué à la protection des données ; rubriques > Ma conformité au RGPD > Passer à l'action > Le délégué à la protection des données (DPO) > Documents associés
- des informations sur la certification des DPD ; rubriques Ma conformité au RGPD > Passer à l'action > Le délégué à la protection des données (DPO) > Certification des compétences du DPO
- le « Guide de sensibilisation au RGPD pour les collectivités territoriales », septembre 2019 ; rubriques Thématiques > Collectivités territoriales > Guide collectivités territoriales

SCHÉMA



Désigner un délégué à la protection des données

OUTIL(S) TÉLÉCHARGEABLE(S)

Outil DTOU6659

Légende de schéma de procédure

FICHE(S) ASSOCIÉE(S)

Fiche 11160

RGPD : se mettre en conformité et le rester – pour tout savoir de vos nouvelles obligations

MODÈLE(S) ASSOCIÉ(S)

Désigner un délégué à la protection des données

© Éditions WEKA - Tous droits réservés

Le Gouvernement promet de renforcer la cybersécurité des hôpitaux

Le Gouvernement lance un vaste programme de préparation aux incidents cyber dans les établissements de santé.

Au cours du second semestre 2022, deux attaques cyber d'envergure ont visé des hôpitaux français. D'abord le CHU de Corbeil-Essonnes, dans l'Essonne, le 21 août 2022, puis le CH de Versailles, dans les Yvelines, le 3 décembre. Ces attaques ont eu des impacts opérationnels importants sur des services hospitaliers déjà en tension. Dans les deux cas, le plan blanc pour les urgences sanitaires graves a été déclenché et certains patients dans les états les plus critiques ont dû être transférés vers d'autres hôpitaux. À la veille de Noël, le ministre de l'Intérieur et des Outre-mer, le ministre de la Santé et de la Prévention et le ministre délégué chargé de la Transition numérique et des Télécommunications ont donc organisé une réunion de travail sur la cybersécurité des hôpitaux. Étaient présents, l'ensemble des services mobilisés et les principales fédérations hospitalières.

À cette occasion, Gérald Darmanin, François Braun et Jean-Noël Barrot ont salué « la réactivité et l'engagement exceptionnel » des professionnels des deux établissements victimes d'une cyberattaque, qui ont permis d'assurer la continuité des soins pour tous les patients dans les meilleures conditions possibles. « Ce type d'attaque démontre à quel point nous devons amplifier collectivement nos efforts, d'autant plus que tous les indicateurs des menaces cyber sont en hausse », ont plaidé les trois ministres.

Ainsi, en 2021, environ 260 000 procédures judiciaires liées au cyber ont été enregistrées par les forces de sécurité intérieure, soit une augmentation de 20 % par rapport à l'année précédente. Dans le même temps, un millier d'attaques au rançongiciel ont été constatées sur le territoire. Enfin, la plateforme Thésée pour la plainte en ligne pour les escroqueries sur Internet, lancée en mars 2022, atteint déjà 75 000 signalements.

Afin de répondre à ces enjeux, la loi d'orientation et de programmation du ministère de l'Intérieur et des Outre-mer, actuellement soumise au contrôle

du Conseil constitutionnel, prévoit de renforcer les moyens en la matière, avec, par exemple, le recrutement de 1 500 cyber patrouilleurs. Dans le cadre de la stratégie d'accélération pour la cybersécurité de France 2030, le Gouvernement mobilise également un programme d'investissement d'1 milliard d'euros. Cette stratégie vise à soutenir le développement d'un écosystème privé de fournisseurs de solutions souveraines et innovantes, qui permettent, notamment, de répondre aux besoins de cybersécurité des établissements de santé.

Depuis près de 2 ans, un « ambitieux » plan de renforcement cyber a été mené : audits des établissements conduits par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), campagne de sensibilisation « Tous cyber vigilants », déblocage de nouveaux financements pour améliorer la sécurisation des logiciels et autres outils techniques…, ont énuméré les ministres. À la suite de la cyberattaque ayant visé le CHU de Corbeil-Essonnes cet été, une enveloppe supplémentaire de 20 millions d'euros a été débloquée pour financer des actions de renforcement du niveau de cybersécurité des établissements de santé.

Afin de renforcer encore davantage la préparation des établissements et leur permettre de faire face en cas d'attaques, les trois ministres ont annoncé, le 21 décembre 2022, le lancement d'un vaste programme de préparation aux incidents cyber. Objectif : que 100 % des établissements de santé les plus prioritaires aient réalisé de nouveaux exercices d'ici mai 2023. Parallèlement, un plan blanc numérique sera élaboré au cours du premier trimestre 2023 pour doter les établissements des réflexes et pratiques à adopter si un incident cyber survient (activation d'une cellule de crise, évaluation des impacts, notamment). Enfin, ce nouveau plan entend mutualiser les ressources compétentes au niveau de chaque région, en lien avec les Agences régionales de santé (ARS).

Gérald Darmanin, François Braun et Jean-Noël Barrot ont réaffirmé que la nouvelle feuille de route 2023-2027 du numérique en santé accordera une place centrale à la cybersécurité des établissements. À cet effet, une task force associant l'ensemble des autorités compétentes est créée pour bâtir, d'ici mars 2023, un nouveau projet de plan cyber pluriannuel massif. Les ministres ont enfin rappelé la posture constante de l'État de non-paiement des rançons lors d'attaque sur les organismes publics. Ils ont aussi insisté sur l'importance de porter plainte systématiquement, afin que des enquêtes puissent être menées et aboutir.

Récemment, un hacker russe au Canada, qui avait participé à plus de 115 attaques contre des victimes françaises, a été interpellé au Canada, se sont félicités le ministre de l'Intérieur et des Outre-mer, le ministre de la Santé et de la Prévention et le ministre délégué chargé de la Transition numérique et des Télécommunications.

En 2021, environ 260 000 procédures judiciaires liées au cyber ont été enregistrées par les forces de sécurité intérieure.

Cybersécurité : prévenir les attaques contre le système d'information hospitalier

Les cyberattaques des hôpitaux de Corbeil-Essonnes et de Versailles ont mis en exergue l'enjeu de la cybersécurité pour les établissements de santé. Le Gouvernement a annoncé fin décembre un plan pour la renforcer. Les hôpitaux peuvent néanmoins déjà prendre des mesures pour l'améliorer. Le point avec Vincent Croisile, expert sécurité à l'ANS, et Emmanuel Sohier, responsable du CERT Santé.

Emmanuel Sohier, responsable du CERT Santé

Vincent Croisile, expert sécurité à l'ANS

Le 21 août 2022, le CHU de Corbeil-Essonnes (91) faisait l'objet d'une cyberattaque d'envergure. Le 3 décembre, c'était au tour du CH de Versailles (78) d'être visé. Dans les deux cas, ces attaques ont eu des impacts opérationnels importants sur les services hospitaliers, nécessitant d'enclencher le plan blanc pour les urgences sanitaires graves et le transfert de certains patients vers d'autres hôpitaux. Ces deux exemples, médiatisés, démontrent l'enjeu que représente la cybersécurité. De fait, le 21 décembre, le Gouvernement a annoncé plusieurs mesures dans ce domaine.

Concernant les hôpitaux, un programme de préparation aux incidents cyber a été lancé pour que 100 % des établissements de santé les plus prioritaires aient réalisé de nouveaux exercices d'ici mai 2023. Un plan blanc numérique doit également être élaboré au premier trimestre 2023 pour doter les établissements des réflexes et pratiques à adopter si un incident cyber survient (activation d'une cellule de crise, évaluation des impacts, etc.).

L'informatique des hôpitaux présente en effet de nombreux risques. « Le système d'information (SI) hospitalier est très complexe et, depuis quelques années, il s'est densifié et comporte de nombreuses applications, explique ainsi **Vincent Croisile, expert sécurité à l'Agence du numérique en santé (ANS).** Il y a aussi la problématique des échanges avec l'extérieur – médecins libéraux ou exerçant dans d'autres établissements – ainsi que le développement du télétravail qui peut étendre la surface d'attaque de l'établissement. La sécurité doit prendre en compte plusieurs éléments : Internet – les flux entrants et sortants, et les accès –, la gestion

des droits et accès en interne, le cloisonnement entre les différents services et applicatifs pour la gestion des droits ».

UN FONCTIONNEMENT DÉGRADÉ

La principale cyberattaque est le rançongiciel. « Un attaquant va réussir à accéder à un système d'information en exploitant des failles ou des vulnérabilités des équipements (Internet VPN, messageries, serveur) mais aussi qui sont propres à la conception du système d'information de l'hôpital, par exemple dans la gestion des droits d'administration, explique **Emmanuel Sohier, responsable du CERT Santé**. En disposant d'un compte, l'attaquant peut alors accéder aux parties du SI les plus critiques comme les sauvegardes. Il chiffre les données et demande une rançon pour que l'hôpital les récupère. Si l'établissement ne paye pas, il peut, dans une deuxième étape, exfiltrer des données afin de faire pression. »

En 2022, le CERT Santé a identifié moins d'une trentaine de cyberattaques liées à un rançongiciel contre des hôpitaux ayant un impact moyen ou fort. Un impact moyen ne touche qu'une partie des fichiers car le système d'information est suffisamment sécurisé. Un impact fort peut impliquer le chiffrement de 80 % des fichiers, y compris de ceux qui servent à gérer le système d'information, avec des conséquences sur les applicatifs métiers. Les équipes et les soignants doivent alors fonctionner en mode dégradé. « Le nombre d'attaques par rançongiciel a diminué de 50 % par rapport à 2021 », précise néanmoins Emmanuel Sohier.

Les cyberattaques à impact fort conduisent cependant à reconstruire le SI hospitalier. « Le principal enjeu est de gérer correctement les différents niveaux de sensibilité du SI, de cloisonner les différentes activités et de mieux sécuriser l'organe central, l'Active directory, qui va gérer l'accès aux différents systèmes et aux applications », détaille Emmanuel Sohier. Concrètement, il s'agit de ne pas reconstruire le SI à l'identique afin de ne pas avoir les mêmes vulnérabilités et failles qu'avant l'attaque.

MAINTENIR LA SÉCURITÉ DU SI

Les hôpitaux peuvent cependant agir afin de prévenir de tels incidents. « La dimension importante pour le gestionnaire du système d'information est de maintenir en condition de sécurité les équipements, en particulier ceux qui sont exposés sur Internet. Les attaques visent en effet les équipements standards. Elles sont le plus souvent massives et ne ciblent pas forcément les hôpitaux », souligne Vincent Croisile. Ce qui signifie notamment de mettre à jour les équipements et les antivirus.

L'identification électronique des utilisateurs constitue aussi un point crucial. Celle-ci doit être à double facteur (un mot de passe et des seconds facteurs d'authentification comme un code à usage unique, un badge…). Un référentiel sur l'identification électronique a été publié et rendu opposable par un arrêté du 28 mars 2022. Il comporte une feuille de route pour les établissements de santé à mettre en œuvre entre le 1er juin 2022 et le 31 décembre 2025.

> Il faut trouver le bon compromis entre les bonnes pratiques en termes de sécurité et le quotidien des utilisateurs.

L'utilisation de messageries sécurisées de santé permet aussi d'augmenter le niveau de sécurité. « Il faut trouver le bon compromis entre les bonnes pratiques en termes de sécurité et le quotidien des utilisateurs. Il est donc nécessaire de bien analyser les risques mais aussi d'intégrer l'enjeu de l'ergonomie pour les utilisateurs afin de ne pas compliquer l'usage des applications et ainsi risquer que les règles de sécurité ne soient pas correctement appliquées », remarque Vincent Croisile.

Enfin, dans le cadre de la vague 2 du Ségur du numérique, l'ANS travaille sur les exigences de sécurité des applications qui seront utilisées par les hôpitaux. L'ANS et le CERT Santé mettent aussi à disposition des établissements de nombreuses ressources tel le corpus documentaire de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

Magali Clausener

FICHE MÉTHODOLOGIQUE WEKA

Fiche 14113

La cybersécurité en établissements de santé, sociaux et médicosociaux

CONTEXTE

L'informatisation et la numérisation croissantes des établissements de santé, sociaux et médicosociaux va de pair tant avec l'amélioration des techniques de prise en charge des patients qu'avec l'augmentation de la vulnérabilité des hôpitaux face au risque cyber. Parce qu'ils traitent des données personnelles sensibles (les données de santé), les hôpitaux représentent une **cible privilégiée** de nombreuses attaques de leurs systèmes d'information (SI). Certains auteurs de cyberattaques n'hésitent d'ailleurs pas à demander une rançon contre la restitution des données volées ou à menacer de les divulguer, ce qui représente dans le même temps un préjudice potentiel important pour les personnes physiques, en l'occurrence les patients, usagers, professionnels de santé et agents publics hospitaliers, auxquels ces données appartiennent.

Le ministère de la Santé, en lien notamment avec l'Agence du numérique en santé (ANS) et l'Agence nationale de la sécurité des systèmes d'information (Anssi), a pu lancer un **plan de renforcement de la cybersécurité en établissement de santé** dans le cadre de la première feuille de route du numérique en santé approfondi dans le contexte de la stratégie nationale d'accélération pour la cybersécurité de « France 2030 » et de la deuxième feuille de route 2023-2027 du numérique en santé.

La cybersécurité à l'hôpital englobe diverses mesures de sécurité pour**protéger les systèmes informatiques, les données, les applications et les réseaux des hôpitaux** contre les menaces informatiques (y compris les virus et les logiciels malveillants), ainsi que des mesures visant à **protéger la confidentialité des données des patients**, y compris le stockage et le transfert sécurisés des données médicales.

▶ 1 - La création préalable d'une stratégie institutionnelle interne de cybersécurité

Les agents hospitaliers, et en particulier les dirigeants d'établissement, doivent avoir une conscience aiguë de la nécessité d'élaborer une stratégie claire et dédiée concernant la protection des systèmes d'information et des données sensibles par la mise en œuvre de mesures de sécurité visant à contrer ou à prévenir toutes sortes d'attaques informatiques. Cela requiert de placer cet enjeu au cœur de la gouvernance en construisant une stratégie adaptée aux particularités de sa structure. La mise en œuvre doit être confiée à une équipe dédiée, généralement rattachée à la direction des systèmes d'information et pouvant inclure des administrateurs réseaux, des juristes et des ingénieurs en informatique.

Il s'agira en premier lieu de s'assurer que les systèmes sont bien conformes dans leurs usages et dans leurs modalités de fonctionnement aux réglementations existantes en matière de protection des données et de confidentialité. Cela implique également un pilotage juridique permettant de veiller à ce que les processus, les applications et les dispositifs informatiques utilisés respectent dans leurs spécifications techniques les dispositions des réglementations applicables prévues par exemple par le règlement général sur la protection des données (RGPD), par le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels (OSE) – dont font partie les 135 groupements hospitaliers de territoire (GHT) – et des fournisseurs de service numérique ou encore par l' ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques de santé concernant l'identification électronique des professionnels de santé inscrits au répertoire partagé des professionnels de santé (RPPS).

Parmi les mesures concrètes de sécurité à prendre, on peut citer la mise en place systématique de pare-feu et de détection automatique des intrusions, de contrôles d'accès pour limiter l'accès aux systèmes logiciels et à Internet, de l'utilisation de mots de passe complexes et uniques pour protéger les comptes et sessions professionnels des agents, d'un système de sauvegarde régulière et de restauration des données de système, du cryptage des données comme l'usage des messageries sécurisées pour les professionnels de santé (MSSanté). Sur ce dernier point, si l'utilisation d'une messagerie professionnelle intégrée à l'espace de confiance MSSanté n'est pas obligatoire en tant que telle, tout professionnel de santé est cependant tenu de respecter le cadre juridique encadrant l'échange des données personnelles de santé (CSP, art. L. 1110-4).

Cette dynamique de stratégie institutionnelle, par nature transversale, doit au moins s'inscrire dans le cadre du projet d'établissement, et sinon dans le cadre d'une stratégie territoriale en lien avec les autres établissements de son territoire, dans le cadre d'un GHT, ou d'un autre type de groupement de coopération quand cela est possible, pour s'assurer d'une mutualisation des ressources à la fois humaine et matérielle et d'un espace de partage des bonnes pratiques en cybersécurité.

▶ 2 - Élaborer une réponse en cas de cyberattaques

Un aspect essentiel de la cybersécurité consiste aussi à savoir quoi faire en cas d'attaque. Cela nécessite d'anticiper les mesures qui seront à mettre en place par la construction d'un processus de gestion des incidents et des plans de réponse aux incidents de sécurité.

Tout d'abord, il convient de s'assurer que l'établissement dispose d'un plan de continuité informatique (PCI) qui doit permettre de garantir, en situation d'incident, une continuité de fonctionnement du système d'information suffisante pour répondre aux exigences de continuité des activités métiers, car une interruption d'une fonction SI peut induire une perte de chance pour le patient. Dès lors, le PCI doit anticiper les situations d'interruption du système d'information et détailler en regard les modalités d'organisation des procédures en fonctionnement dégradé ou en mode « service minimum » (par exemple, définir les durées maximales d'interruption admises et les modalités de reprise progressive après interruption en fonction des différentes contraintes des utilisateurs concernés sur un applicatif informatique et un secteur d'activité donnés) avec les mesures préventives, palliatives et de secours envisagées ainsi que les moyens associés et disponibles pour y parvenir. En outre, le PCI doit être construit en lien avec les autres documents plus transversaux comme le plan de continuité d'activité (PCA) global et les modalités de gestion de crises (plan blanc classique). À ce titre, le guide pratique relatif au PCI de l'Agence du numérique en santé constitue un support utile.

Dans un second temps, il conviendra, conformément à la stratégie 2023-2027 du numérique en santé, de doter son établissement de santé d'un plan blanc numérique recensant les réflexes pratiques à adopter si un incident cyber devait advenir. Pour l'heure, nous savons déjà qu'il existe des délais réglementaires contraints en matière de déclarations à ne pas méconnaître, telles l'information à la Commission nationale de l'informatique et des libertés (Cnil), l'agence régionale de santé, l'Agence du numérique en santé, l'Agence nationale de la sécurité des systèmes d'information, l'information par notification aux personnes physiques dont les données sont concernées par l'attaque (RGPD , art. 40), l'information aux fournisseurs et au procureur de la République (CPP, art. 40).

▶ 3 - La démarche qualité des dispositifs organisationnels et techniques de sécurité des systèmes d'information

L'équipe informatique peut avoir recours à la réalisation d'audits à échéances régulières, internes ou externes en fonction des ressources disponibles, pour vérifier la conformité des dispositifs en place au sein de la structure aux politiques, procédures et réglementations applicables en termes de sécurité informatique. Dans ce cadre, la plateforme oSIS est un exemple d'outil mis à disposition par l'Agence technique de l'information hospitalière (Atih) au service des différents acteurs des systèmes d'information de santé, permettant de suivre l'informatisation des processus de soins et de gestion des établissements de santé, et par le biais duquel les structures peuvent s'autoévaluer et ainsi améliorer, en continu et à leur échelle, la maturité de leur système de sécurité informatique grâce à l'instauration d'une culture de la gestion du risque cyber.

Par ailleurs, l'établissement peut s'engager dans une procédure de certification « hébergeur de données de santé » (HDS) qui repose sur une évaluation de conformité au référentiel de certification de l'Agence du numérique en santé conduite par un organisme accrédité par le Comité français d'accréditation (Cofrac). Le dépôt d'un dossier de demande de certification est possible à deux titres :

- certificat « hébergeur d'infrastructure physique » pour les activités de mise à disposition de locaux d'hébergement physique et d'infrastructure matérielle ;

- certificat « hébergeur infogéreur » pour les activités de mise à disposition d'infrastructure virtuelle, de plateforme logicielle, d'administration/exploitation et de sauvegarde de données externalisée.

La procédure de certification se fonde sur le processus standard de management ISO 17021. Cette démarche permet à l'établissement de santé, après obtention de la certification, d'héberger des données de santé conformément à la réglementation (CSP, art. L. 1111-8) tout en impulsant, en interne, une dynamique de management des systèmes d'information par la qualité.

NOTRE CONSEIL

Les fonctionnaires hospitaliers doivent être conscients des différents risques liés à la cybersécurité et prendre les mesures nécessaires pour les gérer. Une sensibilisation massive des personnels est donc primordiale ; l'établissement devra leur fournir les outils visant à les aider à se protéger aussi individuellement contre les cyberattaques. Pour ce faire, le personnel doit être formé à la compréhension des risques et des menaces liés à la cybersécurité et à la façon d'y réagir.

Souvent, l'humain est le premier facteur de vulnérabilité dans les établissements de santé. C'est la raison pour laquelle il est conseillé de mener une campagne de sensibilisation interne au risque cyber sur le modèle des campagnes de santé publique (exemple de la vaccination). À ce titre, l'Agence du numérique en santé, à travers la campagne « Tous cybervigilants », met à disposition des établissements de santé un kit complet de communication téléchargeable depuis son site Internet.

ALLER PLUS LOIN

Références juridiques

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Code de la santé publique, articles L. 1110-4 et L. 1111-8
- Code de procédure pénale , article 40
- Ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie
- Décret n° 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information
- Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

Bibliographie

- Agence du numérique en santé, *La cybersécurité pour le social et le médico-social en 13 questions*, octobre 2022
- Agence du numérique en santé, *Plan de continuité informatique : principes de base. Guide pratique organisationnel PGSSI-S* , août 2022
- Agence nationale de la sécurité des systèmes d'information, *Guide d'hygiène informatique. Renforcer la sécurité de son système d'information en 42 mesures* , version 2.0, septembre 2017
- Direction générale de l'offre de soins, *Cybersécurité. Connaître vos risques pour mieux y faire face. Mémento à l'usage du directeur d'établissement de santé* , édition 2017
- Ministère de la santé et de la prévention, *FAIT(S), Bilan de la feuille de route du numérique en santé 2019-2022* , juillet 2022

© Éditions WEKA - Tous droits réservés

L'accompagnateur au quotidien des décideurs publics

Depuis 40 ans, Weka met son savoir-faire au service des professionnels des collectivités territoriales et de la fonction publique.

Nous apportons des réponses pratiques et concrètes issues de l'expérience d'experts publics à leurs problématiques quotidiennes, dans les domaines d'intervention suivants :

- Marchés publics
- Finances & comptabilité
- Ressources humaines
- Services à la population
- Culture & communication
- Aménagement des territoires
- Gouvernance locale
- Éducation
- Action sociale
- Santé

.media
.jobs
.fr

Copyright © Éditions WEKA – Tous droits réservés. Février 2023
Toute reproduction ou diffusion partielle ou intégrale des articles de ce numéro est interdite sans le consentement écrit et préalable des Éditions WEKA
Graphiste : Christian LE GALL
Éditrice : Chloé GILLES

Éditions WEKA – Pleyad 1 – 39, boulevard Ornano 93288 Saint-Denis Cedex
Tél. : 01 53 35 17 17 – Fax : 01 53 35 17 01
Site internet : www.weka.fr