MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

HFDS
HAUT FONCTIONNAIRE
DE DÉFENSE
ET DE SÉCURITÉ

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé

Rapport public 2019

SOMMAIRE

TABLE DES FIGURES

1 INTRODUCTION

Le ministère des solidarités et de la santé a mis en place depuis le 1er octobre 2017 un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information des structures de santé.

L'année 2019 a été marquée par une recrudescence de cyberattaques, qui n'ont épargné aucun secteur d'activités, y compris celui de la santé. De nombreux établissements ont subi des attaques, avec parfois des conséquences importantes sur la prise en charge des patients. Ainsi, près de quatre cents incidents ont été signalés au ministère des solidarités et de la santé et soixante-dix demandes d'accompagnements ont été formulées auprès de la cellule cybersécurité en santé, dédiée à l'appui des structures de santé au sein de l'Agence du numérique en santé.

Dans un contexte où la menace continue à se développer et à s'adapter, la cybersécurité à l'échelle de chaque structure de santé est devenue une priorité nationale. Cet enjeu est clairement affiché dans la feuille de route «Accélérer le virage numérique en santé» présentée le 25 avril 2019, où la cybersécurité constitue bien un socle de la transformation numérique en santé et se traduit par le renforcement des mesures sectorielles dans ce domaine.

En 2020, depuis le déclenchement de la crise de la Covid-19, les systèmes d'information jouent un rôle essentiel dans la gestion de l'épidémie. Le développement d'outils numériques spécifiques à disposition des citoyens et des professionnels de santé entraîne des exigences particulières en matière de cybersécurité. La mobilisation des acteurs de la sécurité numérique permet de faire face collectivement à cette situation. Il importe d'en tirer tous les enseignements, afin de renforcer la résilience de notre système de santé.

Les indicateurs présentés dans ce rapport sont le reflet des incidents auxquels les structures de santé qui les ont déclarées ont été confrontées en 2018 et 2019.

Ce dispositif de signalements constitue le premier maillon de la cybersécurité de notre secteur, en contribuant à repérer les attaques avant qu'elles ne se répandent et à renforcer ainsi la capacité de réponse collective ; il est impératif de le faire connaître à l'ensemble des acteurs de la santé.

Au-delà de l'obligation de déclaration, le ministère propose un véritable service aux structures de santé, à la fois dans le cadre du traitement de leurs incidents, mais aussi en vue de renforcer les actions préventives pour en limiter les occurrences. L'enjeu principal est de soutenir et d'accompagner la démarche eSanté, par une démarche de sécurité forte et visible, de nature à apporter la confiance nécessaire aux patients / usagers et aux acteurs de santé.

Le dispositif de prévention et d'alerte ministériel, s'articule autour du portail "cyberveille-sante.gouv.fr", conçu pour informer sur les menaces numériques qui pèsent sur le secteur, donner aux acteurs les clés pour y faire face, et partager les pratiques au sein d'un espace sécurisé. Nous vous invitons à contribuer à la réflexion et à faire part de vos réalisations et de vos attentes, afin d'améliorer ensemble le niveau de sécurité numérique de notre secteur.

Dominique Pon, responsable ministériel du numérique en santé.
Laura Létourneau, déléguée ministérielle du numérique en santé.

2 DISPOSITIF DE TRAITEMENT DES SIGNALEMENTS DES INCIDENTS DE SECURITE DES SYSTEMES D'INFORMATION POUR LE SECTEUR SANTE

2.1 Contexte réglementaire

En application de l'article L. 1111-8-2 du code de la santé publique, les établissements de santé, les hôpitaux des armées, les centres de radiothérapie et les laboratoires de biologie médicale doivent déclarer leurs incidents de sécurité des systèmes d'information depuis le 1er octobre 2017.

Dans le cadre de la mise en application du décret n° 2016-1214 du 12 septembre 2016 (JORF n°0214 du 14 septembre 2016) relatif aux conditions de traitement des incidents graves de sécurité des systèmes d'information du secteur santé, l'Agence du numérique en Santé (ANS) est désignée comme le groupement d'intérêt public (GIP) en charge d'apporter un appui au traitement des incidents de sécurité des systèmes d'information.

L'arrêté d'application du 30 octobre 2017 relatif aux modalités de signalement et de traitement des incidents précise le rôle des agences régionales de santé (ARS) et de l'ANS dans le traitement des signalements et l'accompagnement des structures.

2.2 Présentation des activités

Le dispositif de traitement des signalements des incidents de sécurité des systèmes d'information constitue un élément clé de la stratégie d'amélioration du niveau de sécurité numérique du secteur santé portée par le ministère des solidarités et de la santé, en coordination étroite avec les autorités gouvernementales en charge de la cyber sécurité.

Sa mise en œuvre opérationnelle s'appuie sur la Cellule Accompagnement Cybersécurité des Structures de Santé (ACSS) de l'Agence du numérique en santé. La cellule ACSS a mis en place une démarche méthodique pour améliorer la résilience des structures face aux actes de cybermalveillance.

Mettre à disposition un portail de signalement et proposer un appui

Le traitement des incidents reste de la responsabilité des structures de santé. L'accompagnement et l'appui mis en place par la cellule ACSS dans le cadre de leur signalement consiste à :

- récupérer le signalement sur le portail des signalements des évènements sanitaires indésirables et notifier au déclarant sa prise en compte ;
- analyser et qualifier le signalement pour le compte de l'ARS compétente ;
- apporter, si besoin, un accompagnement dans le traitement de l'incident de sécurité des systèmes d'information ;

- informer le fonctionnaire de sécurité des systèmes d'information (HFDS/FSSI), qui assure le pilotage du traitement en cas d'incident de sécurité majeur (incident de niveau « significatif ») ;
- diffuser 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), dans le cas d'un incident ayant un impact sanitaire ;
- le cas échéant, diffuser une alerte vers les autorités compétentes de l'Etat selon la nature de l'incident :
  - aux agences sanitaires dans le cas d'un incident majeur impactant la prise en charge des patients ;
  - à l'ANSSI, en cas d'incident concernant une structure relevant de dispositifs spécifiques (LPM ou NIS), ou en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs ;
  - à la CNIL en cas d'impact sur les données à caractère personnel.

La cellule ACSS apporte son appui aux structures dans le cadre de la résolution d'un incident :

- orientation vers un prestataire de proximité référencé par le GIP cybermalveillance.gouv.fr dans le cas d'une demande d'intervention sur site ;
- communication de fiches réflexes (ex : phishing, cryptovirus, code malveillant ou défiguration de site Web) ou de recommandations de mesures de remédiation correspondant à la nature de l'incident (ex : changement de mots de passe, mise en liste noire d'adresses de messagerie, blocage de protocoles) ;
- si l'incident a pour origine un maliciel, mise en œuvre d'une analyse de premier niveau de fichiers infectés et de souches virales en vue de proposer des mesures de remédiation.

La cellule ACSS propose aussi un accompagnement dans la phase d'amélioration des mesures de sécurité :

- évaluation technique des plans d'action sécurité :
  - priorisation des mesures proposées (ex : renforcer le cloisonnement réseau du SI support d'activités de soins vitaux) ;
  - propositions pour améliorer la sécurité du SI (ex : utilisation d'une application pour l'administration locale ou pour limiter l'exploitation de vulnérabilités) ;
- rappel des bonnes pratiques d'administration et de développement (ex : promotion des guides de l'ANSSI sur la configuration d'un domaine Active Directory[1] ou la conception d'application web).

[1] L'**Active Directory** (**AD**) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

Animer la communauté « cyberveille-santé »

Le portail cyberveille-santé dispose également d'un espace sécurisé au sein duquel les correspondants cyberveille-santé de la cellule ACSS peuvent échanger entre eux sur :

- des retours d'expérience sur le traitement d'incidents rencontrés et des indicateurs sur les actes de cybermalveillance ;
- les bulletins de sécurité ou les documents publiés sur le portail ;
- les actions ministérielles visant à encadrer et à accompagner les acteurs dans la mise en œuvre de la sécurité numérique.

Cet espace sécurisé a vocation à faciliter les échanges autour de la cybersécurité entre les acteurs du secteur santé.

La cellule ACSS organise périodiquement un webinaire sur les menaces de cybersécurité (attaques à partir de l'Internet, rançongiciels, etc…) et les bonnes pratiques pour renforcer la sécurité des systèmes numériques (exposition sur Internet, cloisonnement, etc…).

Alerter les structures de la menace cyber

Au travers du portail cyberveille-santé dédié à la sécurité du numérique en santé, la cellule ACSS :

- informe et alerte les structures de santé concernant des vulnérabilités ou des dysfonctionnements majeurs de dispositifs médicaux, des technologies de santé ou des technologies standards (système d'exploitation, suite bureautique, base de données, etc...) ;
- alerte les structures de santé concernant des actes de cyber-malveillance (messages électroniques malveillants, rançongiciels, vols de données, etc…) ;
- apporte un appui aux structures dans la gestion de la sécurité et des incidents (fiches réflexes, fiches pratiques, guides de bonnes pratiques).

2.3 Trajectoire

Le Président de la République a présenté en 2018 la politique de transformation de notre système de santé : « Ma Santé 2022 ».

Dans ce cadre, la stratégie nationale du numérique en santé a été annoncée par la ministre chargée de la Santé le 25 avril 2019. Cette stratégie est bien plus qu'une simple ambition, elle est le signe d'une réelle volonté politique et d'un engagement collectif au service des patients, devenus acteurs de leur santé, des professionnels et plus largement de tous les citoyens.

Sous le pilotage de la délégation au numérique en santé (DNS), en découle une feuille de route, qui présente les cinq grandes orientations du virage numérique en santé :

- renforcer la gouvernance du numérique en santé ;
- intensifier la sécurité et l'interopérabilité des systèmes d'information en santé ;

- accélérer le déploiement des services numériques socles ;
- déployer au niveau national des plateformes numériques de santé ;
- soutenir l'innovation et favoriser l'engagement des acteurs.

L'intensification de la sécurité numérique passe par le « Renforcement de la sécurité opérationnelle des systèmes numériques en santé pour garantir la confiance dans la e-santé » (Action 9 de la feuille de route).
En effet, la criticité et la vulnérabilité de nos systèmes numériques en santé face aux cyberattaques imposent de rechercher et de détecter de façon préventive les failles potentielles pour appuyer les établissements. Cela se traduira, à partir de 2020, par :

- l'extension progressive du dispositif de déclaration des incidents de sécurité à l'ensemble des acteurs de santé,
- la mise en place d'un véritable service national de cybersurveillance en santé.

Extension progressive du dispositif de déclaration des incidents

► Pour se prémunir collectivement des risques, tous les acteurs de santé bénéficieront du dispositif de **déclaration des incidents de sécurité**. Cet élargissement a d'ores et déjà été proposé aux EHPAD, qui peuvent ainsi bénéficier de l'appui de la cellule d'accompagnement cybersécurité des établissements de santé.

Mise en place d'un service national de cyber-surveillance en santé

► Prévenir les structures lorsque leurs systèmes sont vulnérables sur Internet

Le service de **cyber-surveillance** réalise à la demande un audit des domaines des structures de santé exposés sur Internet afin de détecter d'éventuelles vulnérabilités.

Pour ce faire, la plateforme de cyber-surveillance mise en place pour le secteur de la santé :

- cartographie et détermine la surface d'attaque d'un système d'information à partir d'Internet ;
- détecte les vulnérabilités qui affectent le système d'information d'une organisation ;
- détecte une éventuelle fuite de données (code-sources, identifiants, données à caractère personnel, etc.) visant le système d'information.

Le rapport de cyber-surveillance fourni à l'établissement présente :

- le périmètre de l'évaluation avec la liste des domaines et sous-domaines, avec une cartographie des systèmes détectés ;
- une synthèse managériale permettant de prendre rapidement connaissance du niveau de sécurité constaté et de la typologie des vulnérabilités ;
- une synthèse technique présentant :

  - les vulnérabilités détectées par niveau de criticité,
  - un plan d'actions de remédiation hiérarchisé ;
- le détail des vulnérabilités identifiées avec pour chacune :
  - la criticité,
  - le type de vulnérabilité (ou catégorie, telle que usurpation d'identité, défaut de configuration, …),
  - le SI affecté,
  - la description de la vulnérabilité,
  - la recommandation associée en vue de sa correction.

Un **observatoire des vulnérabilités** est constitué sur la base d'une consolidation des rapports de cyber-surveillance. L'observatoire présente une analyse de l'exposition sectorielle (benchmark), par typologie de vulnérabilités, par type de structures, …, et mesure son évolution dans le temps.

► Renforcer les échanges avec le portail cybermalveillance

Mis en place au profit des TPE/PME/Citoyen le GIP cybermalveillance identifie des prestataires de proximité vers lesquels les structures peuvent s'adresser en cas d'incidents de sécurité. Cette liste peut utilement être proposée aux structures de santé confrontées à un incident ou à une attaque.

► Intégrer la cellule ACSS de l'ANS au sein du groupe « Inter CERT »

La cellule ACSS se prépare à rejoindre le groupe « InterCERT-FR » qui réunit un ensemble d'organismes ayant des activités d'IRT (Incident Response Team) sur le territoire français. L'objectif est de gagner en visibilité, et de bénéficier des retours d'expérience des membres du groupe et d'échanges bi ou multilatéraux. Cette intégration permettra d'échanger des informations sur les menaces et les vulnérabilités, et d'anticiper les conseils à donner sur le portail cyberveille santé où de lancer une alerte le plus en amont possible.

Renforcement du niveau global de sécurité des établissements de santé

Pour augmenter le niveau global de sécurité du secteur, les structures de santé sont invitées à poursuivre leurs actions de renforcement en matière de sécurité numérique[2].

Ces actions en matière de sécurité numérique et de protection des données s'inscrivent dans une démarche globale de management des risques, visant à améliorer la qualité et la sécurité des soins, et s'intégrant dans les procédures de conformité de l'établissement.

[2] Cf. Plan d'action SSI ministériel (cf. IM SG/DSSIS/2016/309 du 14 octobre 2016) et programme HOP'EN et, pour certains établissements, loi de programmation militaire et directive NIS.

Cette démarche s'appuie sur :

- une gouvernance nationale portée par la DNS, en lien avec le HFDS et la DGOS ;
- une animation territoriale des ARS en matière de mise en œuvre de la politique de sécurité numérique en santé, en s'appuyant sur leurs GRADeS,
- une mise en œuvre opérationnelle par chaque structure, en privilégiant chaque fois que possible les mutualisations, notamment dans le cadre des groupements hospitaliers de territoire (GHT).

Ces mesures s'articulent autour de 4 grands axes :

► Diagnostic :

Réaliser des audits de vulnérabilité des systèmes numériques, et prioritairement sur deux aspects :

- Audit sur l'exposition des systèmes numériques exposés sur Internet ;
- Audit des « Active Directory », colonne vertébrale des SI internes.

► Sécurisation :

Mettre en place un plan d'action spécifique et pluriannuel, à partir des résultats des audits de vulnérabilité, comprenant des mesures immédiates, à 6, 12 et 18 mois.

► Anticipation/ Préparation/ Faire-face

Réaliser des exercices de continuité d'activité, avec la mise en place de procédures de travail en « mode numérique dégradé ».

► Sensibilisation aux risques cybers

Favoriser la prise de conscience et l'adoption de nouveaux comportements par l'ensemble du personnel, au travers d'actions de formation, de sensibilisation et de mises en situation.

Dans ce cadre, une campagne nationale de communication sur la cybersécurité en santé « Tous cyber vigilants » sera lancée à l'automne 2020.

3 Synthèse

En 2019, 300 établissements ont déclaré 392 incidents, soit une augmentation de 20% par rapport à 2018. Le nombre total de déclaration reste encore faible au regard du nombre de structures concernées par l'obligation de déclaration (plus de 3000) et la probabilité qu'au moins la moitié des structures concernées a dû faire face à un incident ayant impacté son fonctionnement normal au cours de l'année.

A la fin de l'année 2018 et à l'issue des 15 premiers mois de mise en œuvre du dispositif, on pouvait déjà observer des tendances sur la nature des incidents auxquels étaient confrontés les structures de santé. Une majorité des incidents (59%) avait pour origine des interruptions de services ou des dysfonctionnements : bugs d'applications métier, défaillances de services opérateur ou de réseaux internes ou même de plateformes d'hébergeurs.

En 2019, le nombre d'incidents d'origine malveillante est en légère augmentation (43%), par rapport à 2018 (41%). On constate une croissance significative des attaques par rançongiciels (+40%) des structures de santé. Cette croissance n'est pas spécifique au secteur santé mais concerne l'ensemble des secteurs d'activité. Certaines structures de petite taille, souvent dépendantes d'un prestataire ne mettant pas en œuvre les bonnes pratiques de cloisonnement des réseaux et de gestion des sauvegardes, ont perdu une grande partie de leurs données à la suite d'une attaque.

Ces attaques, ont aussi visé de façon plus marquante en 2019 des établissements de grande taille, avec des impacts conséquents sur la continuité d'activité de certains services. Le ministère des solidarités et de la santé (HFDS/FSSI) a ainsi été amené à intervenir à plusieurs reprises pour coordonner les actions opérationnelles et de communication avec l'ANSSI, le CORRUSS et les ARS. Ces attaques ont souvent exploité le manque de vigilance des personnels par rapport aux messages malveillants (phishing) et l'exposition sur Internet de services d'accès à distance à des systèmes insuffisamment sécurisés. L'absence de mesures de cloisonnement fort entre les différents domaines métier du SI a aussi facilité la propagation des attaques au sein du SI.

La part des incidents d'origine non malveillante est en légère diminution en 2019 (57%). Ces incidents sont la conséquence de pannes d'opérateurs télécom à l'échelle nationale (en avril et en juin) mais aussi de problèmes locaux (interruptions de service non programmées, dégradations physiques de l'infrastructure). Ces pannes ont affecté l'accès à des services hébergés (dossiers patient informatisés, plateforme de radiologie, résultats de laboratoires, etc…) mais aussi l'accès aux services de téléphonie (service téléphonique de la structure pouvant impacter le SAMU). Les structures disposent souvent de modes dégradés de fonctionnement concernant l'accès aux données via Internet mais plus rarement en ce qui concerne la téléphonie (à l'exception de la régulation des appels pour les services d'urgence), ce qui peut impacter fortement la coordination des soins.

Dans une majorité des cas, les prestataires (opérateurs, éditeurs, hébergeurs) ont apporté une réponse aux incidents dans des délais raisonnables. Les structures ont tout de même été contraintes à mettre en place un fonctionnement dégradé de tout ou partie de leurs activités.

4 TRAITEMENT DES SIGNALEMENTS

4.1 Chiffres clés pour la période 2018-2019

392*	300	70
327*	247	47
		
incidents déclarés sur le portail des signalements	structures ont déclarés au moins un incident	demandes d'accompagnement

14	11	16	8
6	2	15	3
Incidents ont fait l'objet d'un suivi particulier de la part du FSSI	Incidents ont été pris en charge par l'ANSSI	Ont été communiqué à l'ANSM	Incidents ont fait l'objet d'une alerte à la DGS/CORRUSS
HFDS		ansm Agence nationale de sécurité du médicament et des produits de santé	CORRUSS

**Ici sont présentées les données de 2019 en bleu et les données de 2018 en rouge.

Les services du HFDS (FSSI) et l'ANSSI ont particulièrement été sollicités en 2019 dans le cadre d'incidents impactant des structures de grandes tailles. L'ANSSI a aussi été sollicitée pour apporter une assistance à des structures de taille moyenne victimes de rançongiciels.

Les 7 alertes transmises à la DGS/CORRUSS concernaient :

- des incidents d'origine malveillante (arrêt du SI et pertes de données causées par des rançongiciels) ;
- des dysfonctionnements de logiciels de prescription ayant entrainé une suspicion de surdosage ou encore la production de prescriptions erronées.

4.2 Informations générales sur les signalements

Si en 2018, 327 incidents ont été déclarés sur le portail des signalements, l'année **2019** a connu une augmentation sensible avec **392** incidents déclarés.

Parmi les incidents déclarés en 2019, on compte des incidents impactant des pharmacies ainsi que des incidents ne concernant pas des systèmes numériques. Ces incidents n'ayant pas fait l'objet d'un traitement particulier sont au nombre de 38 et n'ont été pris en compte dans les figures 1, 3 et 6.

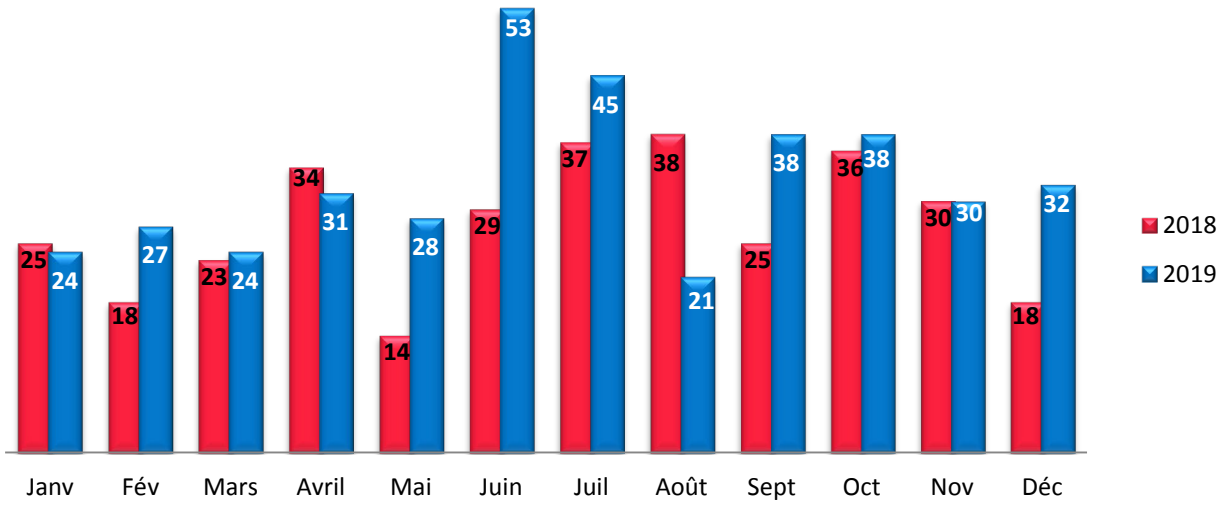

Figure 1 - Nombre de signalements par mois

Par comparaison avec l'année 2018, le nombre mensuel de signalements augmente légèrement en 2019, puisque l'on a en moyenne un peu plus de 32 signalements par mois au lieu de 27. Les deux mois les plus chargés ont été juin et juillet, les structures ayant été touchés par de nombreuses pannes d'opérateurs (locales et nationales).

55 C'est le nombre de structures qui ont déclaré plus de 2 incidents durant l'année 2019 sur 300 établissements au total. Sept d'entre elles ont signalé plus de quatre incidents.

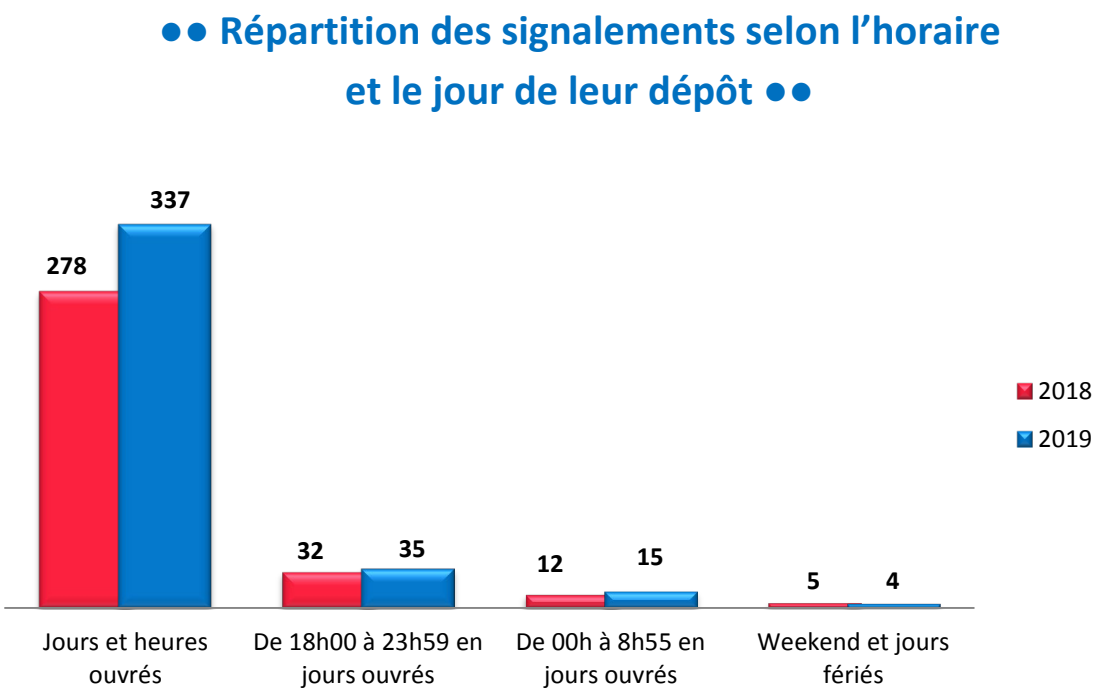

Figure 2 - Répartition des signalements selon l'horaire et le jour de leur dépôt

86% des signalements ont été effectués en jours et heures ouvrés en 2019, entre 9h et 18h.Ce sont principalement des structures publiques qui sont à l'origine des déclarations en dehors de cette période. **11** demandes d'accompagnement ont été formulées en dehors des heures ouvrées dont trois ont concerné des incidents ayant nécessité l'intervention des services du HFDS. Environ 70% des signalements sont réalisés le jour de la survenance de l'incident et 80% dans les 24h.

●● Etat des incidents lors de leur signalement ●●

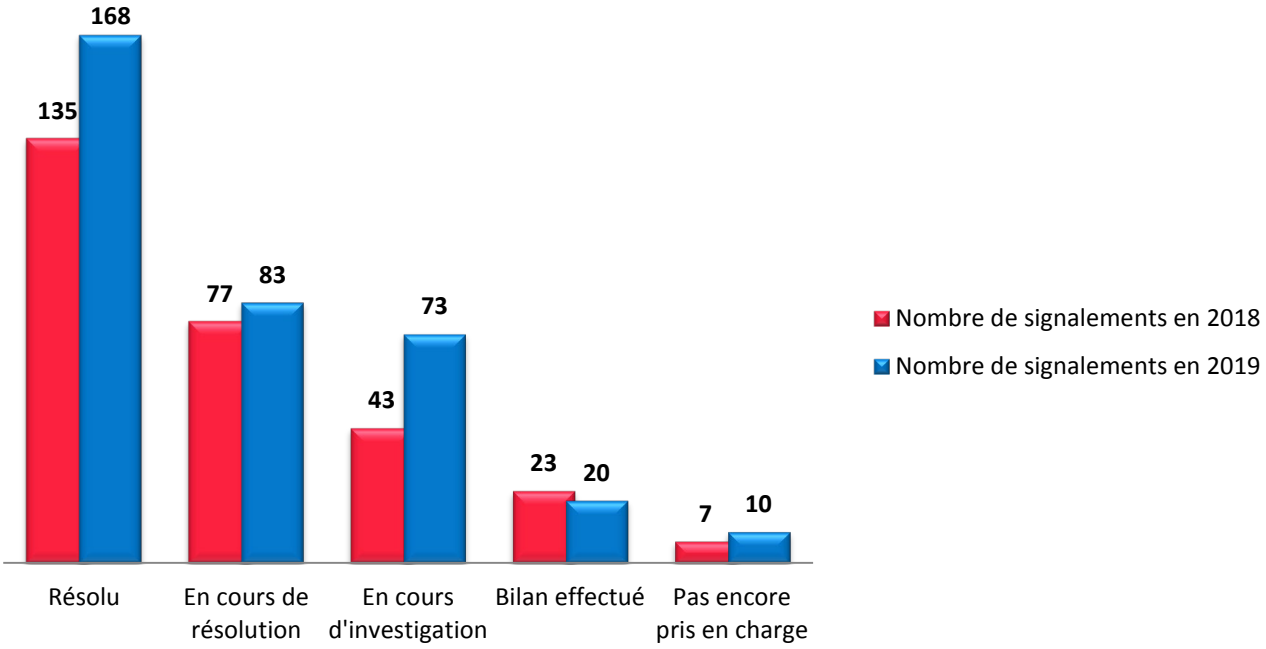

Figure 3 - Etat des incidents lors de leur signalement

Pour la moitié des signalements, l'incident est déjà résolu par la structure lors de sa déclaration, que ce soit en 2018 ou 2019. En revanche, si dans **15 %** des cas, l'origine de l'incident n'a pas encore été identifiée (en cours d'investigation) en 2018, ce chiffre s'élève à **21%** pour l'année 2019.

8 structures n'ont pas donné de suite à leur déclaration malgré une demande de compléments d'information ou une proposition d'appui.

20%

C'est le pourcentage de signalements pour lesquels est demandé un accompagnement. Les accompagnements sont en général demandés lors d'incidents ayant un impact important sur la structure. La principale demande d'appui concerne la gestion des attaques virales et la compromission des systèmes. Mais les structures sollicitent aussi parfois la cellule ACSS pour intervenir auprès de prestataires lorsque ces derniers sont à l'origine de l'incident (panne réseau, dysfonctionnement applicatif) et ne sont pas suffisamment réactifs dans la mise en place de solutions de remédiation.

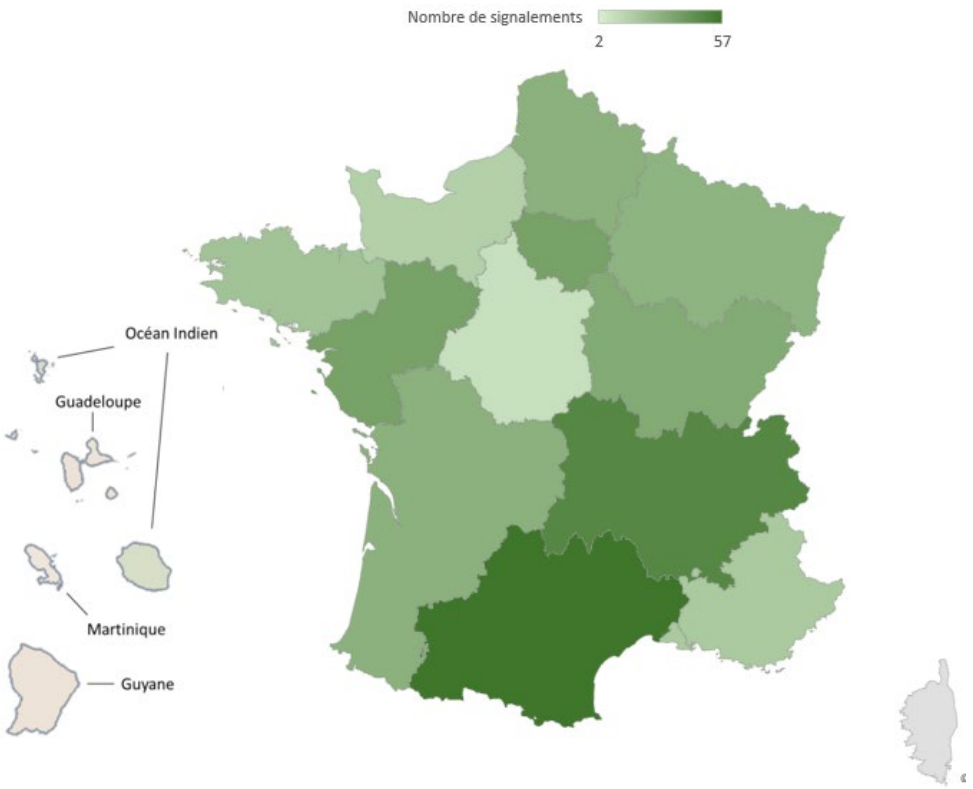

Figure 4 - Répartition des signalements par région

Les régions pour lesquelles le nombre de signalements est le plus important sont Occitanie et Auvergne-Rhône-Alpes avec respectivement 57 et 49 signalements. Ces deux régions représentent à elles seules plus de 28% du total des signalements.

L'ensemble des régions a déclaré au moins un incident.

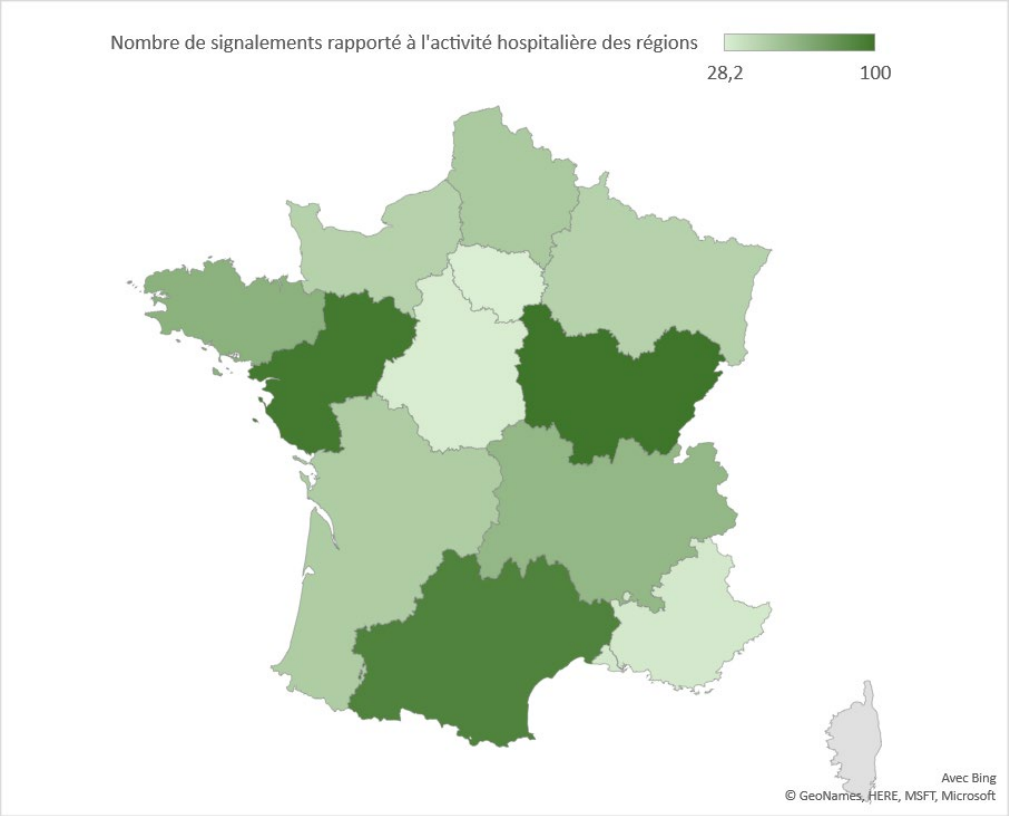

Figure 5 - Nombre de signalements rapporté à l'activité hospitalière des régions

La figure 5 présente le ratio entre le nombre de signalement et l'activité hospitalière rapportée au niveau national : plus une région a un nombre de signalements élevé par rapport à son activité, plus celle-ci est foncée. Les DOM-COM n'ont pas été pris en compte dans cette analyse à cause du faible taux d'activité hospitalière par rapport à la métropole. La région avec ce ratio le plus élevé (Bourgogne-Franche-Comté) est utilisée en tant qu'indice 100.

Au regard de son activité hospitalière (4.41% de l'activité nationale soit presque quatre fois moins que l'Île-de-France), la Bourgogne-Franche-Comté est en tête en matière de remontée des incidents.

●● Répartition des signalements selon le type de structure ●●

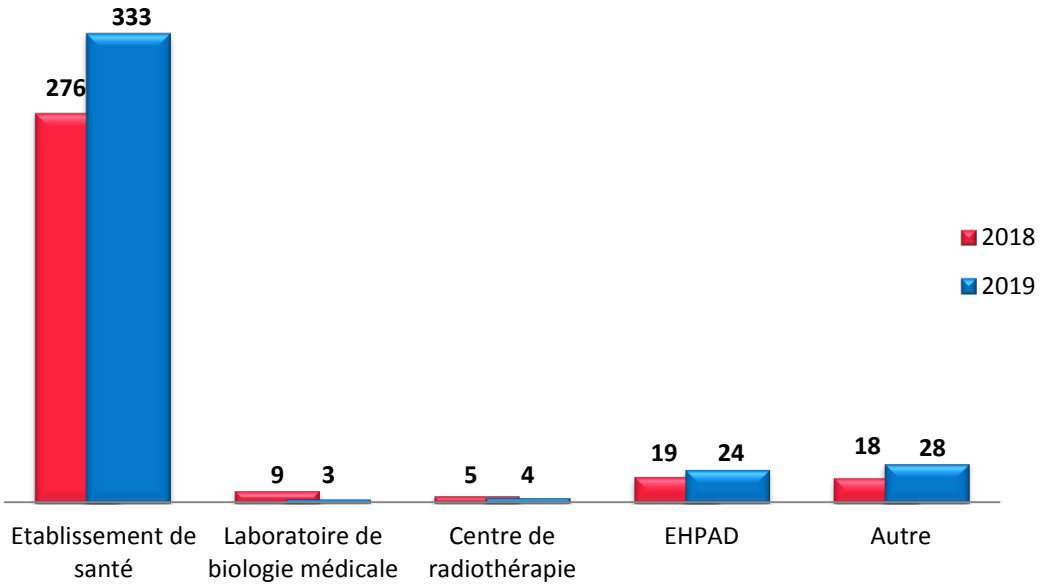

Figure 6 - Répartition des signalements selon le type de structure

La majorité des signalements est déclarée par les établissements de santé (85% en 2019). En 2019, on constate une baisse concernant les laboratoires de biologie médicale et une augmentation de la déclaration de structures n'étant pas dans l'obligation de déclarer : EHPAD et la catégorie « Autres » qui correspond principalement à des déclarations réalisées par des pharmacies, des cabinets libéraux et des établissements publics du secteur médico-social.

●● Part des signalements comparée à la part des établissements selon leur type ●●

Les établissements publics sont toujours largement majoritaires dans la déclaration des incidents. Il y a toujours une sous-déclaration des incidents par les acteurs du privé. Ces structures qui ont dû parfois faire face à des incidents importants sont encore peu enclines à partager les informations concernant leur gestion.

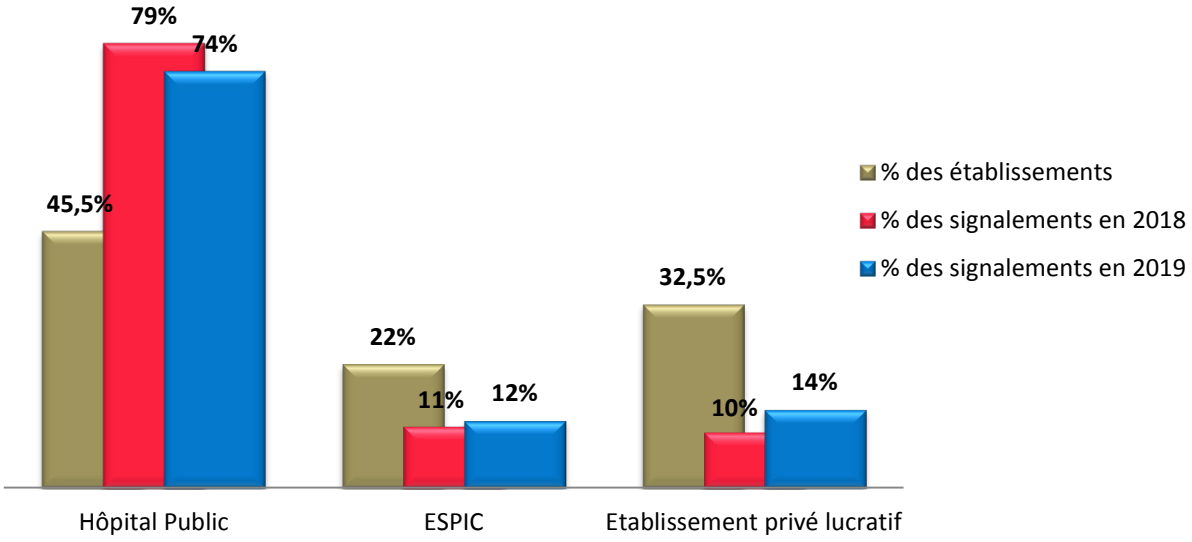

Figure 7 - Part des signalements comparée à la part des établissements selon leur raison sociale

**PSPH : Participant au Service Public Hospitalier / *ESPIC Etablissement de Santé Privé d'Intérêt Collectif*

Les actes malveillants

La technique du phishing constitue toujours en 2019 le vecteur d'attaque privilégié pour déployer un code malveillant sur un système ciblé. Le manque de vigilance ou la négligence est souvent à l'origine de la compromission : réponses à des messages électroniques malveillants ou accès à des sites web malveillants.

Les attaquants ont également exploité deux autres types de vulnérabilité pour déployer leurs rançongiciels :

- des failles de sécurité (OS, logiciels, progiciels ou matériels non patchés) ;
- l'accès à distance à des systèmes Windows avec des mots de passe peu complexes.

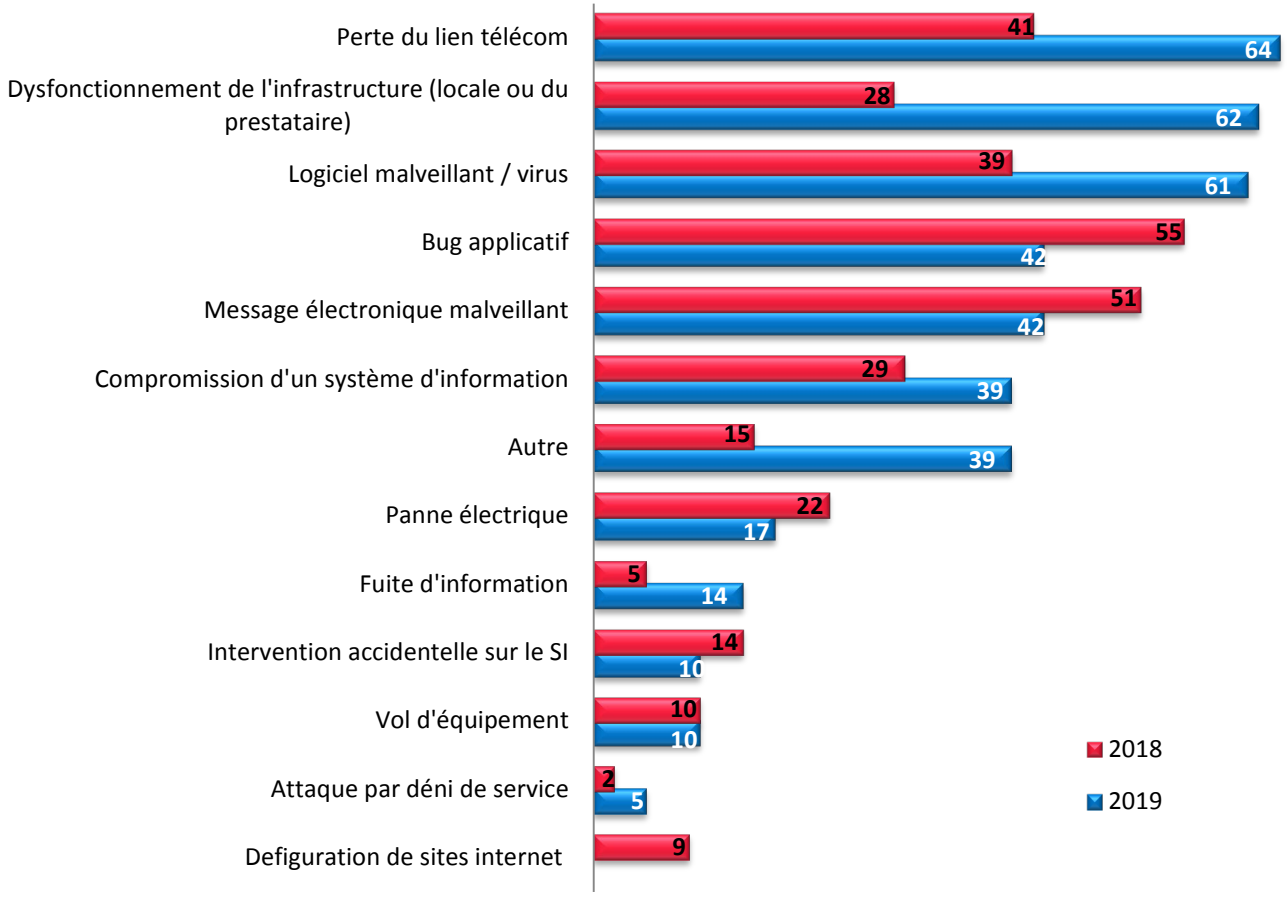

Figure 8 - Nombre d'incidents par type d'origine

Après avoir restauré les systèmes et les données impactées, une majorité des structures de santé n'a ni le temps, ni l'expertise ou les moyens financiers pour rechercher méthodiquement la porte d'entrée utilisée par l'attaquant.

Les codes malveillants ayant le plus affecté les structures de santé sont les rançongiciels. Les structures ont été victimes de variantes de rançongiciels connus comme Locky (2018), Dharma et Gandcrab (2018 – 2019) ou Phobos et Emotet (2019). Certains sont déployés manuellement par l'attaquant, d'autres se déploient automatiquement (comme des vers) sur l'ensemble des machines appartenant à un même domaine Windows. Certains rançongiciels n'ont pas été détectés par les solutions antivirales du marché.

Le montant de la rançon n'est pas précisé systématiquement dans le message de l'attaquant. Il est demandé de plus en plus fréquemment à la structure de prendre contact avec une adresse mail. Pour la majorité de ces rançongiciels, il n'existait pas d'outil de décryptement/déchiffrement au moment de l'incident.

Lorsque les rançons sont explicitement formulées, elles peuvent s'élever à une dizaine de milliers d'euros. Ces sommes sont similaires à ce que l'on observe dans différents secteurs d'activité. De plus, les modalités d'attaque et de demande n'étant pas individualisées ni spécifiques au secteur santé, il est fort probable qu'elles ne visaient pas des établissements en particulier. A notre connaissance, seules deux structures du secteur privé ont payé la rançon demandée pour récupérer leurs données.

Durant ces deux années, des vieilles souches virales comme Wanacry et Conficker ont aussi réapparues. En conservant des machines avec des systèmes obsolescents au sein de leur SI, certaines structures augmentent la probabilité d'être confrontées à des sinistres majeurs.

Les fuites d'information correspondent à la perte de confidentialité de données. Elles ont principalement pour origine des erreurs dans la configuration des matériels ou des logiciels ou des mésusages de droits d'accès à des dossiers patients.

Aucune défiguration de site Internet n'a été signalée en 2019.

La catégorie « Autre » concerne principalement des incidents d'origine malveillante et correspond à des tentatives d'escroquerie par téléphone ou par fax visant à récupérer des informations confidentielles (identifiants ou données à caractère personnel) ou extorquer des fonds.

43% C'est le pourcentage en 2019 des incidents qui ont une origine malveillante, avec comme principaux vecteurs de déclenchement, les messages électroniques malveillants et les logiciels malveillants / virus. Ce chiffre est stable par rapport à 2018.

Les signalements d'origine non malveillante

En 2018, les bugs applicatifs ont constitué la première menace non malveillante à laquelle ont été confrontées les structures de santé. Les logiciels les plus impactés par ces bugs étaient les logiciels d'aide à la prescription et à la dispensation, engendrant des erreurs dans les prescriptions médicales et la délivrance des médicaments. En 2019, les logiciels de dossiers patients informatisés ont eux aussi été particulièrement impactés.

Dans une majorité des cas, les éditeurs ont apporté des correctifs dans des délais compatibles avec la mise en place temporaire de mesures de vigilance exceptionnelles pour éviter de commettre des erreurs dans la prise en charge des patients. Cependant, dans certains cas, minoritaires, les demandes répétées des structures de santé n'ont pas été prises en compte par les éditeurs et ont affecté durablement l'activité des professionnels de santé.

La deuxième cause importante des signalements non malveillants en 2018 a concerné la perte du lien télécom : perte d'accès à Internet ou coupure de la ligne téléphonique. Dans cette situation, les structures ont pu être isolées (perte de liaison au sein d'un GHT, avec les cabinets de ville, avec des fournisseurs, …) et n'avaient plus accès aux services et données dont elles avaient besoin quotidiennement (dossiers patient informatisés, plateforme de radiologie, résultats de laboratoires, etc…). Certains établissements ont fait remonter des difficultés avec les opérateurs de téléphonie. En effet, en plus des difficultés à joindre les services support, ils ont été confrontés aux délais d'intervention peu compatibles avec la disponibilité requise par la mission de prise en charge des patients.

Déjà importants en 2018, le volume d'incidents déclarés en 2019 à cause d'une perte télécom en fait la première cause de signalements d'incident. On dénombre plusieurs pannes de réseau au niveau national ou au niveau local (souvent dû à des dégradations des supports physiques (fibre) mais aussi de coupures non programmées ou des saturations de matériels de raccordement).

Le dysfonctionnement de l'infrastructure (locale ou du prestataire) support du SI est aussi en nette augmentation en 2019 par rapport à 2018. Cela concernait principalement des interruptions de service des applications hébergées, des systèmes de stockage, des dysfonctionnements de serveurs (DPI, base de données) et des systèmes de gestion d'appels malades.

57% C'est le pourcentage en 2019 des incidents qui ont une origine non malveillante, chiffre en légère baisse par comparaison à 2018, avec 59%.

●● Répartition des déclarations selon le type d'impact sur les données ●●

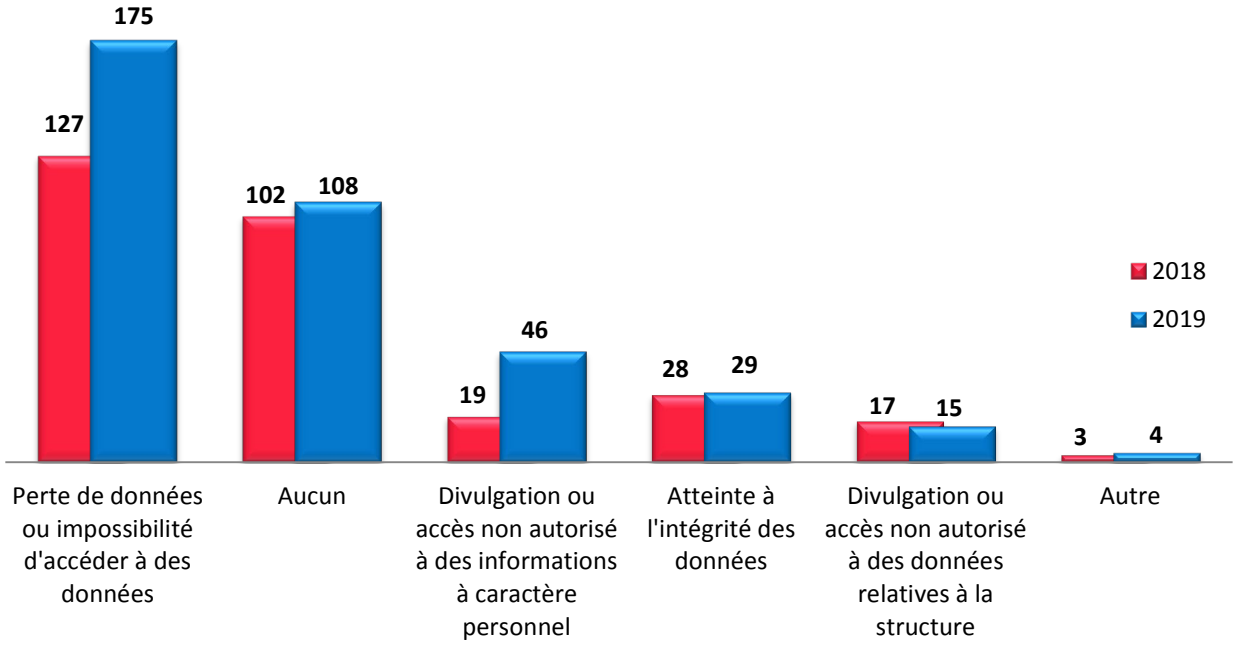

Figure 9 - Répartition selon les types d'impact sur les données

Pour la moitié des incidents signalés en 2019, tout ou partie des données présentes sur le SI de la structure n'étaient plus accessibles. Lorsque l'origine de l'incident était malveillante, ceci était principalement dû à un rançongiciel.

Pour 30% des signalements, les structures assurent qu'il n'y a eu aucun impact sur les données. Cependant, dans de nombreux cas, l'incident signalé a pour origine une perte du réseau téléphonique ou des tentatives de phishing.

●● Evolution du nombre d'incidents d'origine malveillante ●●

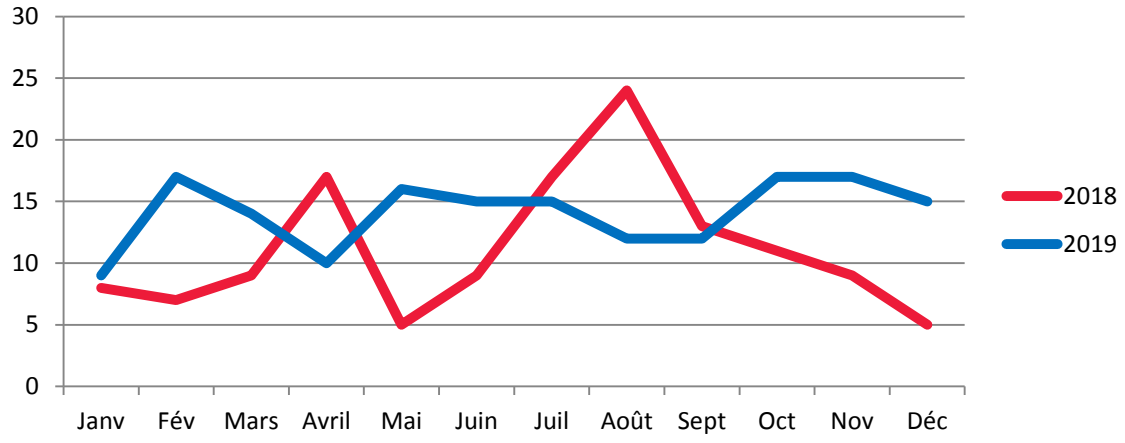

Figure 10 - Evolution du nombre d'incidents dont l'origine est malveillante

Contrairement à 2018 dont la courbe est particulièrement irrégulière, l'année 2019 affiche une relative stabilité mensuelle dans les déclarations des incidents ayant une origine malveillante. Au même titre que les autres secteurs, les structures de santé ont été la cible d'actes de cybermalveillance tout au long de l'année.

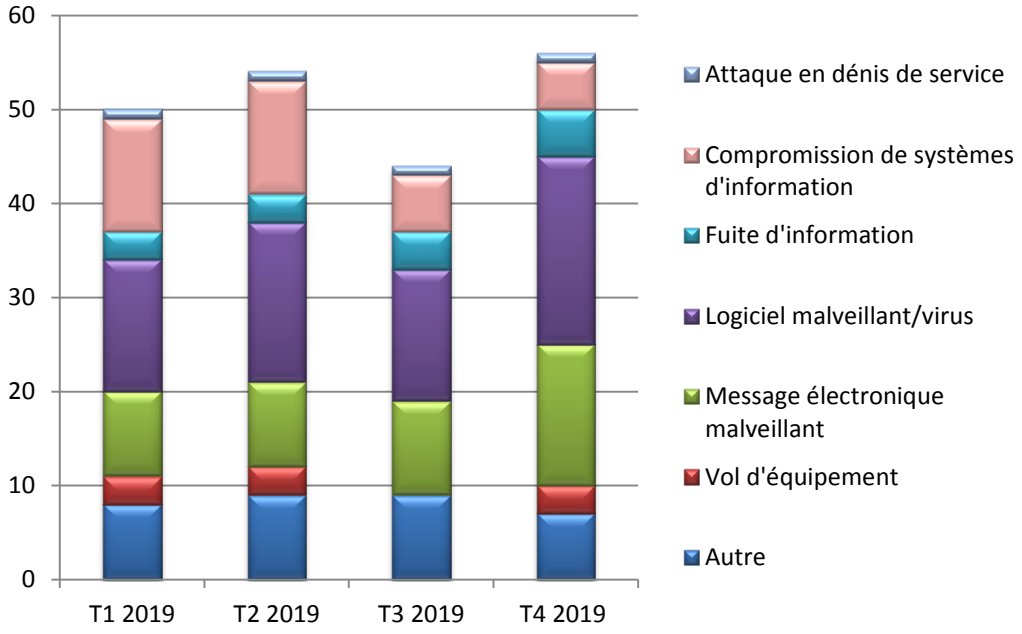

Figure 11 - Origine malveillante des incidents par trimestre

Evolution du nombre d'incidents d'origine non malveillante

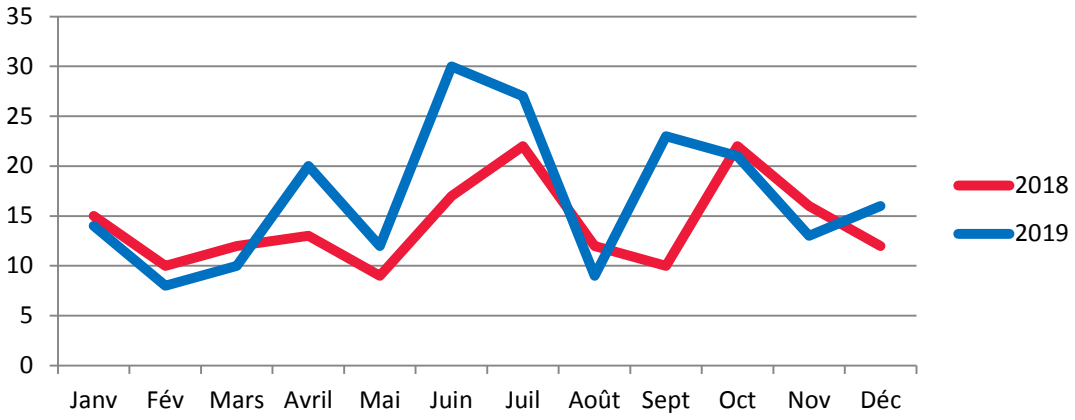

Figure 12 - Evolution du nombre d'incidents dont l'origine est non malveillante

La perte de l'accès à Internet (perte du lien télécom) constitue l'incident le plus fréquent. Cette perte peut fortement impacter le fonctionnement des activités métier des structures de santé : dossiers patients, télétransmissions de scanners, accès à des résultats de biologie, flux avec l'EFS, messagerie, etc… De nombreuses structures ont signalé une interruption de services de plus de 4h et quelques-unes de plus d'une journée. Peu de structures ont les moyens de disposer d'une ligne de secours totalement indépendante du lien primaire. Des actions pourraient être menées au niveau national sur les engagements de services des opérateurs afin d'obtenir une meilleure qualité de prise en charge en cas d'incidents.

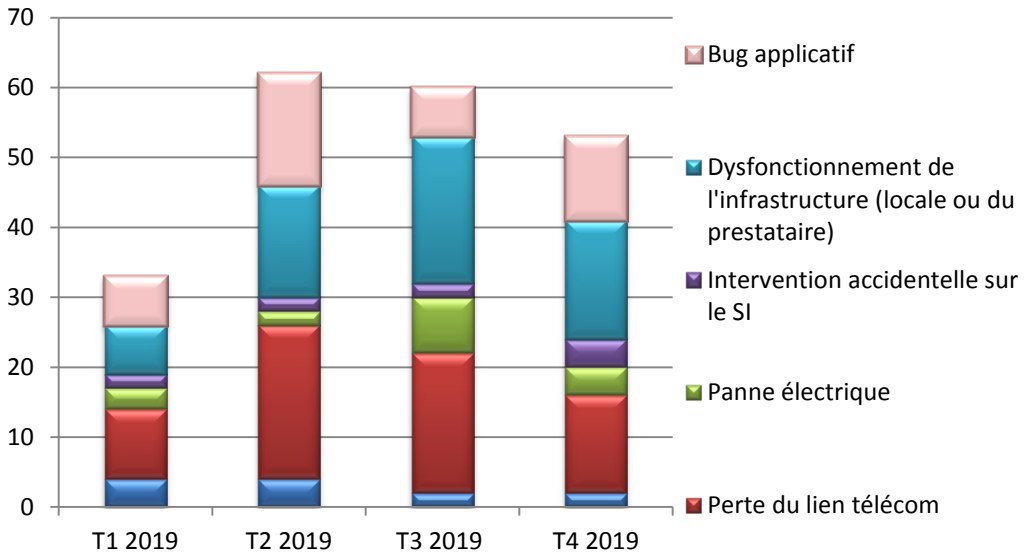

Figure 13 - Origine non malveillante des incidents par trimestre

40%

C'est le pourcentage de structures qui ont été contraintes à mettre en place en 2019 un fonctionnement en mode dégradé du système de prise en charge des patients (en légère baisse par rapport à 2018). Ce mode dégradé dépend de la nature de l'incident et des procédures mises en place dans les structures : application du plan de continuité, utilisation du mode de fonctionnement papier pour gérer les patients, utilisation d'un poste dédié, mise en place de solutions de contournement pour prendre en compte les dysfonctionnements des logiciels de prescription, etc... En moyenne, le mode dégradé a été mis en œuvre par les structures de santé sur une journée mais certains établissements ont été confrontés à cette situation pendant plusieurs jours.

Mise en danger potentielle des patients

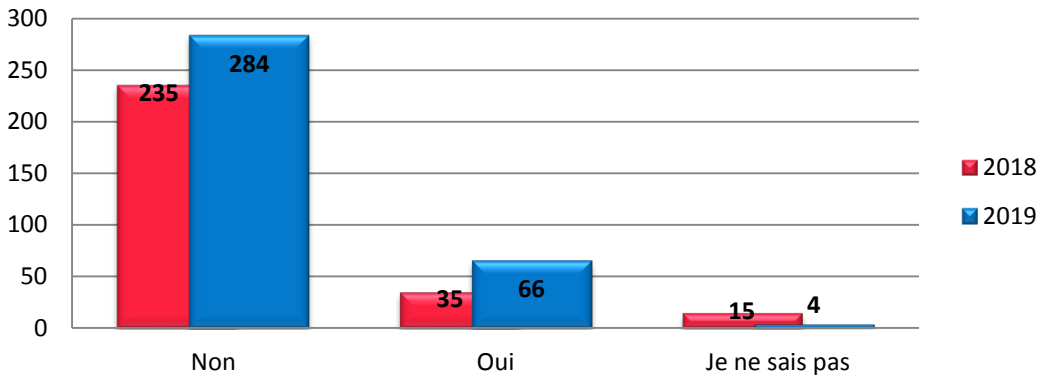

Figure 14 - Mise en danger potentielle des patients

Parmi les 66 mises en danger potentielles en 2019 (19%), 5 incidents ont entrainé une mise en danger patient avérée : prescription incomplète ou erronée (3 cas ; dans l'un des cas, une patiente n'a pas reçu la totalité de son traitement personnel pendant 10 jours, entraînant une détresse respiratoire grave sur OAP), surdosage d'insuline et surdosage de traitement anticoagulant. Ces conséquences sur la prise en charge des patients sont dues à des :

- bugs sur des logiciels de prescription et d'aide à la dispensation impactant l'intégrité des prescriptions et des dispensations ;
- bugs sur des logiciels de dossier patient informatisé ;
- dysfonctionnements de l'infrastructure locale.

Les dysfonctionnements des logiciels de prescription/aide à la dispensation liés à des bugs ayant provoqué des erreurs dans les prescriptions et la délivrance des médicaments auraient pu entrainer une mise en danger des patients plus importante sans la vigilance des professionnels de santé et la mise en place de procédures permettant d'identifier les erreurs.

38% C'est le pourcentage de structures indiquant que l'incident n'a eu aucun impact sur son fonctionnement en 2019. Ce chiffre est relativement stable puisqu'il était de 35% en 2018.

4.3 Incidents notables ayant fait l'objet d'un retour d'expérience anonymisé

Plusieurs incidents déclarés ont fait l'objet d'un retour d'expérience publié sur l'espace sécurisé du portail. Ces retours d'expérience ont permis de faire la lumière sur le mode opératoire de certaines attaques et de présenter les mesures de remédiation à mettre en œuvre en cas d'incident.

Parmi ces incidents, on peut signaler :

- une intrusion via un service d'accès à distance à un contrôleur de domaine Windows utilisé par un prestataire exposé sur Internet suivi du déploiement d'un cryptovirus ayant chiffré l'intégralité des données liées aux activités support (partage de fichiers) et impacté cette activité pendant 24h;
- une intrusion via un service de bureau à distance Windows exposé sur Internet suivi du déploiement d'un cryptovirus ayant chiffré l'intégralité des données en production et des sauvegardes et ayant entrainé un arrêt complet du SI pendant 9 jours.

Ces incidents ont permis de rappeler l'importance de :

- mettre en place une surveillance particulière des accès à distance sur le SI (y compris ceux des prestataires) et de veiller à une gestion des mots de passe à l'état de l'art ;
- limiter les actions possibles depuis le réseau au dépôt de fichiers (système de sauvegarde en ligne) dans le respect du principe de moindre privilège (accorder uniquement le droit de suppression des fichiers de sauvegarde à un administrateur local des serveurs).

4.4 Publication d'alertes sur le portail cyberveille-santé

En 2019, plusieurs alertes ont été publiées sur le portail cyberveille-santé du fait de l'augmentation du nombre d'actes de cybermalveillance et à des dysfonctionnements pouvant impacter des structures de santé.

Faisant le constat d'une augmentation significative au premier trimestre 2019 des attaques par rançongiciel des structures de santé et des pertes irréversibles de données liées à une mauvaise gestion des sauvegardes, une alerte rappelant les bonnes pratiques en matière d'isolation et de contrôle des accès aux sauvegardes a été publiée début avril 2019.

Après le signalement d'un CHU en avril 2019 faisant état du blocage de 500 postes à la suite d'une mise à jour de Windows et sur lesquels était installé le logiciel anti-virus Sophos Endpoint, la cellule ACSS a publié une alerte recommandant de retarder la mise à jour des postes dans l'attente de la correction de l'anomalie par l'éditeur. Il a aussi été proposé un mode opératoire pour redémarrer les postes dans le cas où la mise à jour aurait déjà été réalisée.

Enfin, à la suite de nombreux signalements d'incidents de sécurité dus à la compromission de serveurs de messagerie Zimbra en mai 2019 (possibilité de téléverser un fichier et d'exécuter un code arbitraire), une alerte a été publiée pour recommander la mise à jour urgente des serveurs basés sur cette technologie. Il a aussi été rappelé la nécessité d'une restauration préalable du système pour s'assurer qu'aucun fichier malveillant ne puisse subsister après l'installation du correctif.

4.5 Observatoire des vulnérabilités

Les incidents de sécurité liés à des actes de cybermalveillance sur des services numériques accessibles sur Internet et les audits réalisés dans le cadre du service de cyber-surveillance accélèrent la prise de conscience des structures sur les risques encourus en exposant trop de ressources sur Internet.

Il est possible de réduire une part importante des risques identifiés avec des solutions peu couteuses et faciles à mettre en place**. La rationalisation des ressources exposées est en l'état l'action prioritaire à entreprendre par les structures de santé**.

Six axes d'amélioration ont été mis en évidence pour le périmètre **des services numériques exposés sur Internet**. Les principales recommandations découlant de ces audits sont :

- **réduire les surfaces d'attaque** : certaines structures de santé auditées exposent un grand nombre de services numériques sur Internet. Il a ainsi été démontré la possibilité de prendre le contrôle total de serveurs ;
- **améliorer le suivi des correctifs** : des structures de santé exposent sur internet des systèmes avec des composants obsolètes. Il est indispensable d'assurer une veille des composants exposés sur internet et de les mettre à jour suivant un processus éprouvé lorsque des correctifs sont disponibles. La priorité doit être donnée aux correctifs de sécurité correspondants à des vulnérabilités critiques afin de se prémunir au plus vite d'attaques cherchant à les exploiter ;
- **renforcer la configuration et la sécurisation des accès** : beaucoup de failles détectées lors des audits concernent une mauvaise configuration des protocoles utilisés (par exemple le protocole SSL/TLS utilisé dans le cadre d'échanges chiffrés https) ou une divulgation d'informations sensibles. L'ensemble de ces vulnérabilités peut être corrigé assez simplement par la mise en œuvre de bonnes pratiques ;

- **vérifier la suppression des failles web classiques (présentées dans le Top 10 OWASP[3])** : se conformer aux bonnes pratiques de développement (par exemple le contrôle des saisies utilisateur). Il peut également être mis en œuvre un web application firewall (WAF) qui bloquera l'essentiel des tentatives d'exploitation des failles référencées par l'OWASP s'il est correctement configuré ;
- **limiter l'indexation par les moteurs de recherche de vulnérabilités** : parmi les ressources exposées, nombreuses sont celles identifiées par les moteurs de recherche en ligne spécialisés dans la découverte de vulnérabilités. Il est donc recommandé de bloquer au niveau des firewalls le référencement des ressources exposées sur internet par ces moteurs de recherche, afin de se prémunir de ce type d'attaques ;
- **inclure des engagements sur le maintien en condition de sécurité des équipements gérés par des prestataires** : de nombreuses vulnérabilités critiques ont été ainsi découvertes sur des systèmes gérés par des tiers externes. Lors de la contractualisation d'une prestation avec un tiers, il est essentiel d'inclure des engagements sur le maintien en condition de sécurité.

[3] Le Top 10 OWASP est un document de sensibilisation standard pour les développeurs et la sécurité des applications Web. Il représente un large consensus sur les risques de sécurité les plus critiques pour les applications Web.

5 GLOSSAIRE

ACSS	Accompagnement Cybersécurité des Structures de Santé
ANS	Agence du numérique en santé
ANSM	Agence Nationale de la Sécurité du Médicament et des produits de santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information
ARS	Agence Régionale de Santé
ASIP Santé	Agence des Systèmes d'Information Partagée de Santé
Code malveillant	Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau. Remarques : Les virus ou les vers sont deux types de codes malveillants connus.
CORRUSS	Centre opérationnel de réception et de régulation des urgences sanitaires et sociales
Cryptovirus	Rançongiciel - Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Le terme « rançongiciel » (ou ransomware en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon.
Cybermalveillance	La cybermalveillance recouvre toute activité criminelle réalisée par le biais d'Internet et des technologies du numérique. Elle englobe toute forme de malveillance effectuée à l'aide de l'informatique, d'équipements électroniques et des réseaux de télécommunication.
Cybersécurité	État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.
DGS	Direction Générale de la Santé
DNS	Délégation au numérique en santé
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information

HFDS	Haut Fonctionnaire de Défense et Sécurité
LDAP	Lightweight Directory Access Protocol
Phishing	Hameçonnage - Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.
RGPD	Règlement Général sur la Protection des Données

NOTES PERSONNELLES

Pour aller plus loin, rendez-vous sur :

- le site du Ministère des Solidarités et de la Santé : solidarites-sante.gouv.fr
- le site de l'Agence du numérique en santé : esante.gouv.fr
- le portail cyberveille : cyberveille-sante.gouv.fr/

Pour prendre contact :

- au sein du Ministère des solidarités et de la santé :

  ssi@sg.social.gouv.fr

- au sein de l'Agence du numérique en Santé :

  cyberveille@sante.gouv.fr

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

HFDS
HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

AGENCE DU NUMÉRIQUE EN SANTÉ