AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

CERT Santé

Observatoire des signalements d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social

Rapport public 2023

SOMMAIRE

TABLE DES FIGURES

1 INTRODUCTION

L'observatoire du CERT Santé permet chaque année de partager l'évolution de la menace cyber et la qualité de la réponse collective. L'année 2023 a été marquée par une activité malveillante importante avec une augmentation sensible des attaques par rançongiciel et des vols d'identifiants. Non spécifiquement ciblé, le secteur de la santé est comme de nombreux autres confronté à la professionnalisation des attaquants.

Les ES et ESMS ont dû faire face à ce contexte de menace cyber. Plusieurs victimes de ces attaques ont été contraintes de fonctionner en mode dégradé pendant plusieurs jours et à engager des travaux de refonte partielle ou totale de leur système d'information. Ces situations ont conduit les professionnels à revoir leurs pratiques, générant du stress et de la fatigue. De nombreux établissements ont également subi d'importantes fuites de données des patients. Ces différents dommages ont occasionné des dépenses importantes liés à la gestion de l'incident, à la perte d'activité et la reconstruction du SI. Et ils continuent de démontrer la criticité du pilier cyber dans la pérennité et la confiance dans le développement de la e-santé (et la mise en œuvre de la feuille de route 2023-2027 du numérique en santé).

Avec la conviction que la menace cyber continuera à croitre, en termes de « motivation », d'intensité et de « qualité », il est primordial que l'ensemble des acteurs -puissance publique, établissements et industriels- poursuivent et augmentent leur investissement dans la cybersécurité.

Dans le cadre des programmes CaRE et Segur du numérique vague 2, la Délégation au numérique en santé (DNS) impulse une nouvelle dynamique pour renforcer la résilience des ES face aux menaces de cybersécurité, dans laquelle l'ANS est pleinement impliquée sous ses différentes composantes -pilotage de programme, CERT Santé, régulation, accompagnement des industriels et des régions-. Cette nouvelle gouvernance mobilise l'ensemble des parties prenantes en impliquant les niveaux nationaux (ANS, ANSSI, DGOS, DNS, HFDS), régionaux (ARS et GRADeS), locaux (professionnels, établissements) mais également les acteurs de l'écosystème (fédérations hospitalières et médico-sociales, industriels).

Les établissements de santé doivent pouvoir s'approprier, décliner et déployer le programme CaRE au cœur de leur projet d'établissement et le rendre visible au travers de leurs choix stratégiques et budgétaires, à quelques mois de la mise en œuvre de NIS2.

Les entreprises de service numérique contribuent aussi directement à la résilience des établissements contre les actes de cybermalveillance et doivent aussi s'emparer des enjeux cyber dans leur stratégie et leur plan produit.

Bonne lecture et poursuivons cette mobilisation collective.

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

2.1 Contexte réglementaire et organisationnel

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 à l'Agence du Numérique en Santé (ANS) qui est désignée comme le groupement d'intérêt public (GIP). Depuis le 18 novembre 2020, cette obligation a été étendue aux établissements médico-sociaux par ordonnance n° 2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé (ARS).

Le décret d'application n°2022-715 du 27 avril 2022 précise le rôle et les missions de l'ANS, en particulier son périmètre d'intervention en matière d'appui à la réponse à incident et les actions de prévention.

Ces missions sont portées au sein de l'ANS par le CERT Santé, premier CERT sectoriel en France ayant intégré en janvier 2021 l'InterCERT FRANCE. L'InterCERT FRANCE est une association loi 1901 qui constitue la première communauté de CSIRT[1] en France. Le CERT Santé coopère avec les autres CSIRT/CERT dans l'analyse des menaces de cybersécurité et partage ses retours d'expérience. Il bénéficie régulièrement de l'activité de veille des membres de la communauté (indicateurs de compromission, fuite d'identifiants, etc…).

2.2 Présentation des activités

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

Sa mise en œuvre opérationnelle s'appuie sur le CERT Santé de l'Agence du Numérique en Santé depuis sa création en 2017.

[1] Computer Security information Response Team

Mise à disposition d'un portail de signalement et proposition d'un appui

L'accompagnement et l'appui mis en place par le CERT Santé dans le cadre de leur signalement consiste à :

- Traiter 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 des autorités compétentes ;
- Apporter, si besoin, un accompagnement dans le traitement de l'incident de sécurité des systèmes d'information ;
- Diffuser une alerte vers le ministère des solidarités et de la santé et/ou les autorités compétentes de l'Etat selon la nature de l'incident :
  - le fonctionnaire de sécurité des systèmes d'information des ministères sociaux (FSSI), qui assure le pilotage du traitement en cas d'incident de sécurité majeur ;
  - 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 ;
  - 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 (OIV ou OSE), ou en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs.

Le CERT Santé apporte son appui aux structures dans le cadre de la réponse à un incident :

- Proposition des mesures de confinement complémentaires au cours d'un premier entretien (isolation des sauvegardes, restriction des flux entrants/sortants, isolation de l'Active Directory[2], désactivation massive de comptes, etc…) ;
- Assistance à l'identification de la menace et le scénario complet de la compromission (acquisition et analyse de journaux d'évènements et de preuves numériques, analyse de codes malveillants, de fichiers infectés, recherche du « patient 0 » de l'attaque, etc…) ;
- Proposition de mesures de remédiation adaptées (désinfection des systèmes compromis, suppression des fichiers malveillants, correction des vulnérabilités exploitées, etc…) ;
- Orientation vers un prestataire cyber dans le cas d'une demande d'intervention sur site.
- Mise à disposition de fiches réflexes (ex : maliciel, hameçonnage 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) ;

Le CERT Santé propose aussi un accompagnement dans la phase d'amélioration des mesures de sécurité (notamment dans le cadre d'une procédure de durcissement post-incident):

- Proposer et émettre un avis sur des plans d'action sécurité :

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

- 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) ;

▶ Proposer des solutions pour renforcer la sécurité (configuration des systèmes, solutions concrètes de sécurisation des sauvegardes, hyperviseurs, de l'administration, du cloisonnement réseau, etc…) basées sur les guides de l'ANSSI.

Le traitement des incidents reste la responsabilité des structures déclarantes.

Permanence 24/7

Depuis octobre 2022, le CERT Santé assure un service de réponse à incident aux heures non ouvrées, soit 24h/24 et 7j/7. Une astreinte est joignable au 09 72 43 91 25 pour apporter un appui dans la qualification de l'incident et la mise en œuvre de mesures permettant de stopper la propagation d'une activité malveillante au sein du système d'information d'un bénéficiaire du CERT Santé.

Publication d'alertes sur la menace cyber et partage de bonnes pratiques

Au travers du portail cyberveille-santé dédié à la sécurité du numérique en santé, le CERT Santé :

▶ Informe 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 en cours de réalisation (campagne de messages électroniques malveillants, 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).

Veille proactive

Depuis 2020, le CERT Santé alerte par message électronique les établissements de santé ou les établissements et services médico-sociaux concernant :

- la présence d'une ou plusieurs vulnérabilités critiques sur leur(s) système(s) exposé(s) sur Internet et faisant l'objet de campagne d'exploitation ;
- la compromission potentielle ou avérée de comptes de messagerie ou de comptes d'accès à distance sur des machines exposées sur Internet ;
- les services sensibles exposés sur Internet (RDP, DICOM, etc…)

Cette activité d'alerte est réalisée en étroite coopération avec le CERT-FR de l'ANSSI. Pour les machines concernées, ces alertes précisent l'adresse IP, le nom de domaine et le ou les services.

Service de cybersurveillance

L'audit de cybersurveillance est un service de diagnostic et d'évaluation de la sécurité du système d'information vis-à-vis d'Internet (service national de cybersurveillance). Le service de cybersurveillance réalise un audit des domaines et sous-domaines exposés sur Internet déclarés par la structure[3] afin de détecter d'éventuelles vulnérabilités.

Le service de cybersurveillance permet, pour un périmètre de domaines exposés sur Internet défini, de :

- cartographier et déterminer la surface d'attaque d'un système d'information ;
- détecter de manière pro-active les vulnérabilités qui affectent le système d'information.

L'audit se déroule en deux phases :

- Une phase passive consistant en la collecte d'informations à partir de sources ouvertes sur Internet ;
- Une phase active consistant en la réalisation d'un audit de chacun des domaines du système d'information de la structure. Cette phase comprend :
    - Une cartographie des services et des ressources accessibles ;
    - L'utilisation des scanneurs généralistes / spécifiques afin de détecter d'éventuelles erreurs de configuration et / ou des défauts de mise à jour ;
    - Le test des comptes avec des identifiants faibles et des identifiants par défaut.

Une fois le diagnostic réalisé, un rapport d'audit est fourni à la structure auditée dans des délais courts afin de lui permettre de rapidement mettre en place les éventuelles mesures de remédiation.

Le périmètre de l'audit ainsi que les attendus du rapport sont présentés sur le portail cyberveille-santé[4]. Ces informations permettent d'encadrer les audits de cybersurveillance lorsqu'ils sont réalisés par des prestataires à la demande des structures.

Animation de la communauté « CERT Santé »

Le CERT Santé dispose d'un salon Tchap au sein duquel les RSSI, DSI et les acteurs étatiques de la cybersécurité en santé peuvent échanger entre eux sur :

- L'état de la menace ;
- Des bonnes pratiques et la mise en œuvre de solutions ;
- 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.

---

[3] A l'occasion de ce cadrage, le CERT Santé peut détecter des domaines ou sous domaines non déclarés par la structure

[4] https://cyberveille-sante.gouv.fr/cybersurveillance

Améliorer la sécurité de la messagerie

L'utilisation de courriels malveillants (technique de l'hameçonnage) est très développée par les attaquants pour chercher à compromettre un SI. Le CERT Santé propose aux structures de tester les règles de sécurité de leur serveur de messagerie avec un service en ligne. Ce service a pour but d'identifier les améliorations à apporter dans la configuration des règles de sécurité de la messagerie pour réduire le risque de manipulation de contenus malveillants par les utilisateurs. Il permet de vérifier que la politique de contrôle des messages et de leur contenu a pris en compte les principales menaces issues de l'émetteur, de métadonnées du message (en-tête, encodage, découpage en plusieurs parties, etc…), d'une pièce jointe (spam, virus, etc…), d'une URL (hameçonnage), etc. … Le service contient plus de 170 points de contrôle.

3 Synthèse de l'activité en 2023

Le nombre total d'incidents déclarés (581 signalements) reste relativement stable par rapport à 2022 (592), ainsi que la part des incidents qui sont d'origine malveillante (50%). Parmi les 462 établissements ayant déclaré au moins un incident, soit une augmentation de 9% du nombre de déclarants par rapport à 2022, 93 ont bénéficié d'un appui technique de la part du CERT Santé.

Cette stabilité du nombre d'incidents déclarés et la part des incidents d'origine malveillante peut être la conséquence de deux tendances qui s'opposent :

- Des actions visant à faire baisser le nombre d'incidents d'origine malveillante :
  - une meilleure prise en compte des alertes transmises par mail par le CERT Santé, en particulier lorsque des campagnes d'exploitation de vulnérabilités critiques ont été identifiées ;
  - Une maturité des ES qui progresse sensiblement avec une amélioration de la sécurité de l'exposition sur internet mais encore de façon trop insuffisante par rapport au niveau de la menace (une forte impulsion est donnée et attendue [5]par le programme CaRE dans le cadre du Domaine D1).

- un contexte favorable à leur augmentation :
  - une activité malveillante importante en 2023 comme le rappelle le récent rapport de l'ANSSI sur le panorama de la cybermenace de 2023 indiquant une recrudescence des attaques malveillantes, de la part d'acteurs mieux armés et très motivés par l'appât du gain ;
  - une plus grande sensibilité des ES à la déclaration, mais avec encore une marge de progression comme le met en évidence les indicateurs régionaux.

La menace rançongiciel reste la plus importante en 2023 en termes d'impact sur le SI. Le nombre d'incidents lié à cette menace est en hausse de 10% par rapport à 2022 et concerne majoritairement des établissements et services médico-sociaux ainsi que quelques établissements de santé privés. Le chiffrement des données était souvent précédé d'une exfiltration faisant l'objet d'une mise en vente sur Internet. Ces établissements ont été contraints de mettre en place un mode dégradé de fonctionnement qui pouvait s'étendre sur plusieurs semaines.

Plus de la majorité des incidents sont déclarés par les établissements de santé publics (56%). Les ES publics sont donc les plus nombreux à déclarer un incident au regard du ratio qu'il représente par rapport à l'ensemble des établissements sanitaires. Ce constat peut être expliqué par les éléments suivants :

- Une plus grande activité hospitalière avec un nombre important d'interconnexions avec l'extérieur impliquant une plus grande exposition ;
- Les établissements de santé publics étant mieux sensibilisés à la déclaration des incidents d'origine cyber que les établissements privés, il est possible que le nombre

[5] Arrêté du 18 mars 2024 relatif à un programme de financement destiné à renforcer la sécurité numérique des établissements de santé - Fonction « Annuaires techniques et exposition sur internet » - Légifrance (legifrance.gouv.fr)

d'incidents les concernant soit plus proche de la réalité, comparé aux établissements privés.

Aucun n'élément tangible ne permet d'affirmer qu'il existe une différence de maturité entre les types d'établissements ou alors que certains soient plus spécifiquement ciblés.

Le nombre d'incidents ayant un impact sur la prise en charge des patients est toujours important mais reste stable par rapport à 2022. En effet, 203 signalements en 2023, comme en 2022, indiquent que les établissements ont été contraint de passer en mode dégradé ou d'interrompre la prise en charge des patients soit 35% des signalements reçus ; seuls 25% de ces incidents ont une origine malveillante, les 3 causes principales étant la perte de lien télécom, un bug applicatif généralement sur le DPI ou un dysfonctionnement de l'infrastructure locale ou prestataire.

Ce constat renforce la nécessité de travailler sur les PCA-PRA afin de minimiser l'impact de ces incidents sur la prise en charge des patients. Cette problématique est intégrée dans l'un des prochains domaines du programme CaRE.

L'année 2023 a également été marquée par une diminution sensible des incidents majeurs.

En outre le nombre d'incident d'origine malveillante ayant un effet extrême ou important sur le système d'information de l'établissement victime[6] a diminué : il y en avait 22 en 2022 contre 17 en 2023.

Ceci peut s'expliquer comme suit :

- Un service de veille pro-active du CERT Santé plus efficace avec l'envoi d'alertes dans des délais très courts suite au lancement de la campagne d'exploitation ;
- Un plus grand nombre d'établissements a réalisé un audit de l'exposition sur Internet et réduit sa surface d'attaque ;
- De nombreux établissements de santé ont engagé en 2023 des travaux visant à améliorer ou mettre à jour leurs processus de PCA / PRA et/ou ont réalisé des exercices de crise[7] ;
- Une capacité organisationnelle et technique des établissements de santé à réagir plus vite, dès la détection qui s'illustre par : des points de contact dans la plupart des établissements, des équipes opérationnelles, et une capacité à mettre à jour les infrastructures dans des délais très courts.

Enfin, le CERT Santé est intervenu en 2023 auprès de 8 prestataires de solutions métier suite à l'identification de vulnérabilités présentes sur des serveurs exposés sur Internet. Ces vulnérabilités ont été identifiées soit lors d'un audit de cybersurveillance, soit lors de la réponse à un incident. Le CERT Santé a pu accompagner certains éditeurs dans la correction des vulnérabilités ainsi que dans le renforcement de la sécurité de leur application et de leur infrastructure.

[6] Compromission majeure, exfiltration de données et dommages durables sur le SI

[7] https://esante.gouv.fr/strategie-nationale/cybersecurite

4 OBSERVATOIRE DES SIGNALEMENTS

4.1 Chiffres clés pour la période 2022-2023

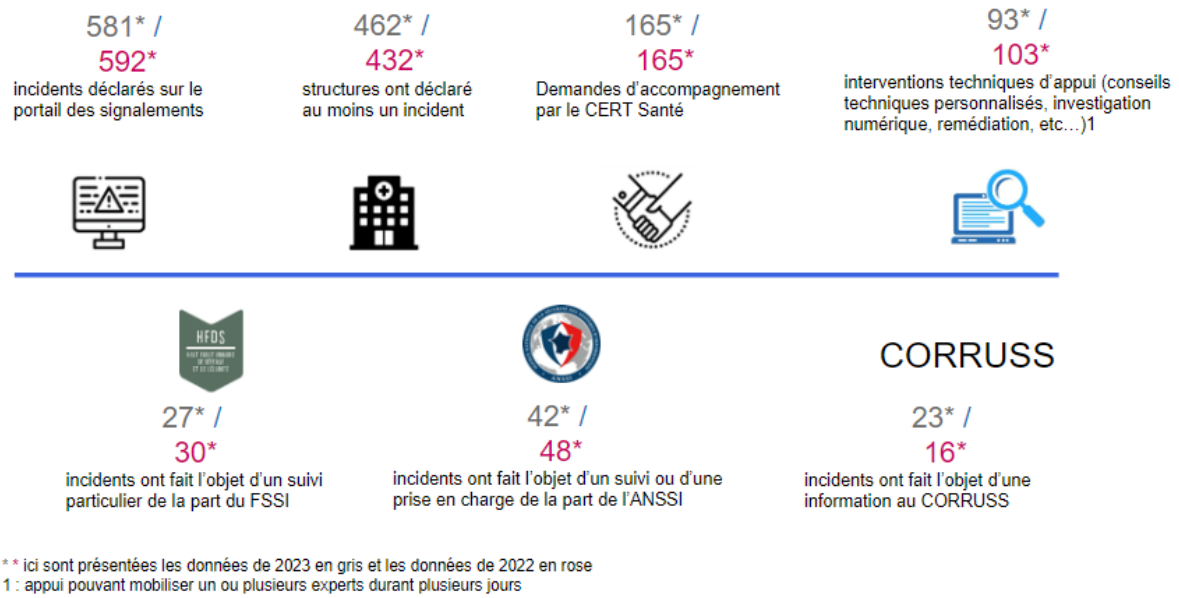

Figure 1 – Chiffres clés des signalements déclarés en 2022 et 2023

En coordination avec le CERT Santé, l'ANSSI et le FSSI sont intervenus directement au profit de 40 établissements, dans le suivi de la gestion d'un incident ou l'appui à la réponse. Certaines structures ont bénéficié de plusieurs interventions et le FSSI est intervenu auprès de certains prestataires sectoriels.

Pour **l'ANSSI** il s'agit de :

- Vingt-huit établissements de santé publics, dont 24 opérateurs de services essentiels (OSE). Ces incidents étaient liés à des attaques par rançongiciel, des compromissions de comptes (AD, VPN ou messagerie), l'exploitation de vulnérabilités sur des équipements de sécurité ou des dysfonctionnements graves de systèmes critiques ;
- Cinq établissements de santé privés et quatre établissements de service médico-sociaux victimes de rançongiciels, de compromission de comptes (AD, VPN ou messagerie), d'exploitation de vulnérabilités ;

Pour le FSSI du MSS, il s'agit de :

- Vingt-trois établissements dont 14 OSE. Ces incidents étaient liés à des attaques par rançongiciels, à la compromission de SI et aux dysfonctionnements graves de systèmes critiques, et pertes du lien télécom.

●● Evènements marquants de la période ●●

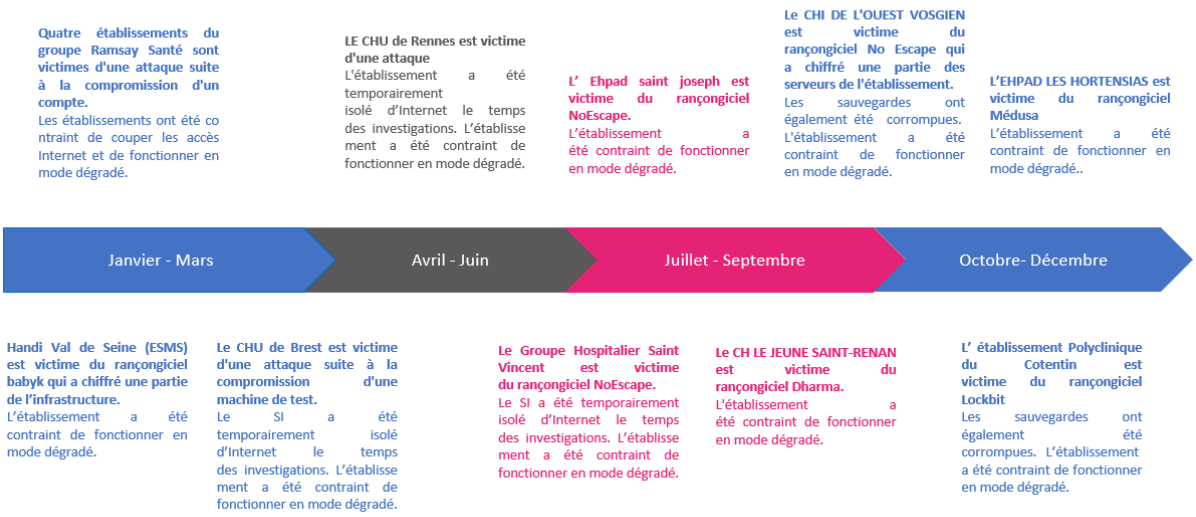

Figure 2 – Evènements marquants de l'année 2023

4.2 Informations générales sur les signalements

581 incidents ont été déclarés en 2023. Ce nombre est en légère baisse par rapport à 2022 (592). Pour mémoire, 733 incidents avaient été déclarés en 2021.

Parmi ces incidents, on compte des incidents « hors périmètre » (24 au total). La majorité des incidents non traités par le CERT Santé sont des incidents ne concernant pas un système d'information support d'une activité sanitaire ou médico-sociale. On comptabilise également dans cette catégorie les exercices de crise cyber qui intègrent une déclaration de l'incident au CERT Santé (3).

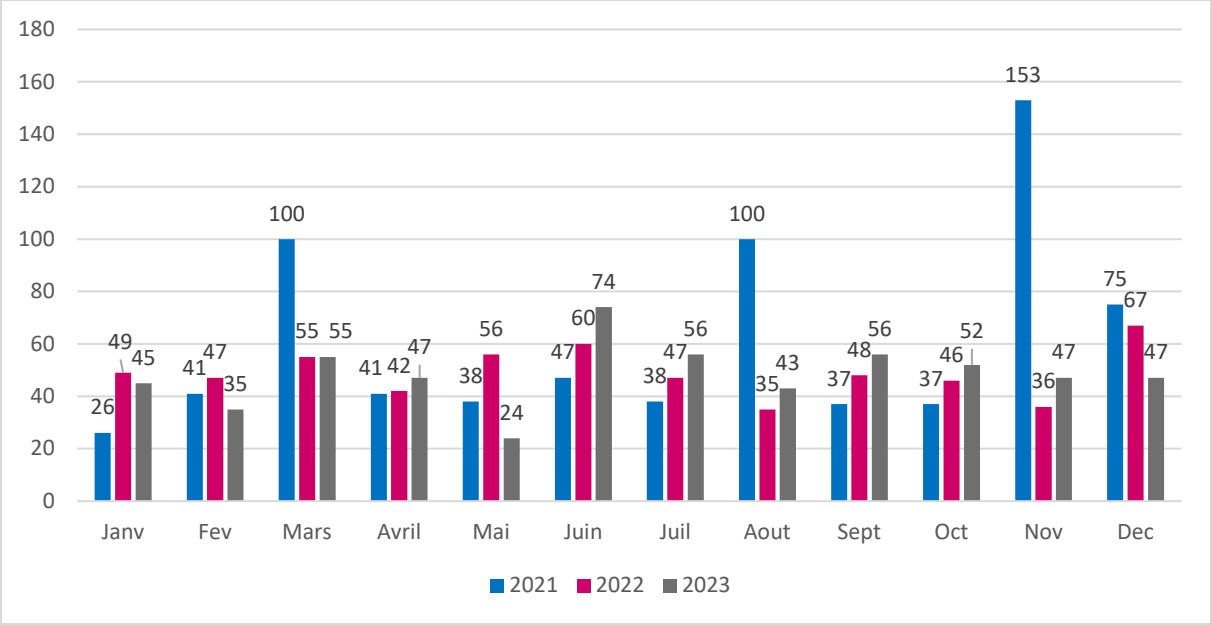

Figure 3 - Nombre de signalements par mois

On compte en 2023 une moyenne de 48 déclarations par mois (49 en 2022).

●● Répartition des signalements selon l'horaire et le jour de leur dépôt ●●

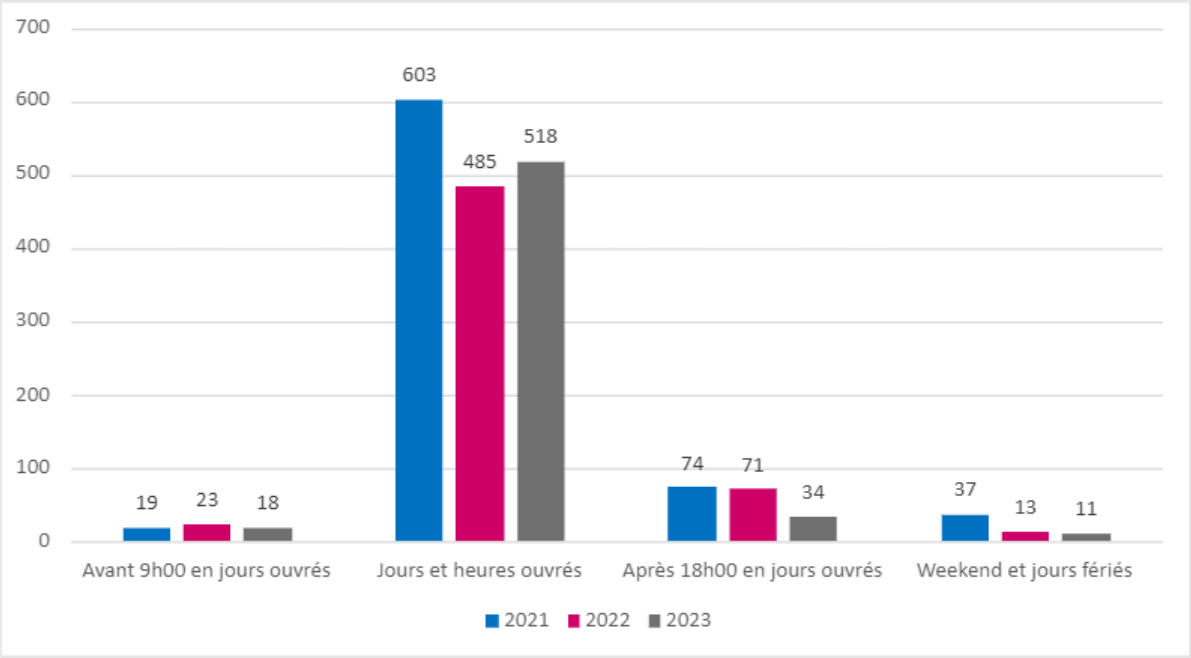

Figure 4 - Répartition des signalements selon l'horaire et le jour de leur dépôt

89% des signalements ont été effectués en heures et jours ouvrés (HO/JO) en 2023, entre 9h et 18h, en augmentation de 15% par rapport à 2022. On constate cependant une augmentation significative des incidents déclarés entre 18h et 18h30 alors qu'en 2022 une grande part des incidents déclarés en HNO étaient déclarés après 20h.

Ce sont principalement des structures publiques qui sont à l'origine des déclarations en HNO/JNO sur le portail des signalements. Vingt-cinq demandes d'accompagnement ont été formulées durant ces périodes. Parmi celles-ci, douze structures (cinq CH, deux hôpitaux privés à but non lucratif, un hôpital privé, une association, un groupe de laboratoires de biologie médicale et deux EHPAD) nécessitaient un appui suite à des attaques par rançongiciel entraînant un fonctionnement dégradé des activités support ou du système de prise en charge des patients, à des compromissions de comptes AD ou de messagerie, ou à des exploitations de vulnérabilités. Deux demandes d'accompagnement en HNO/JNO ayant fait l'objet d'un appui technique se sont avérées être des faux-positifs. Elles ont été prises en charge rapidement par le CERT Santé. Elles ont également bénéficié d'un appui de l'ANSSI et ont fait appel à un prestataire spécialisé dans la réponse à incident et la reconstruction d'un SI post-incident pour les appuyer sur place.

13 incidents ont été pris en charge en 2023 par **l'astreinte du CERT Santé** suite à un appel téléphonique en HNO. 12 ont fait l'objet d'un appui technique en heures ouvrées.

Il est nécessaire de prendre en compte que la déclaration formelle d'un incident au CERT Santé n'est néanmoins pas toujours opérée par le même service que celui responsable de sa détection. Aussi, il n'y a pas de corrélation directe entre l'horaire de détection d'un incident et celui de sa déclaration.

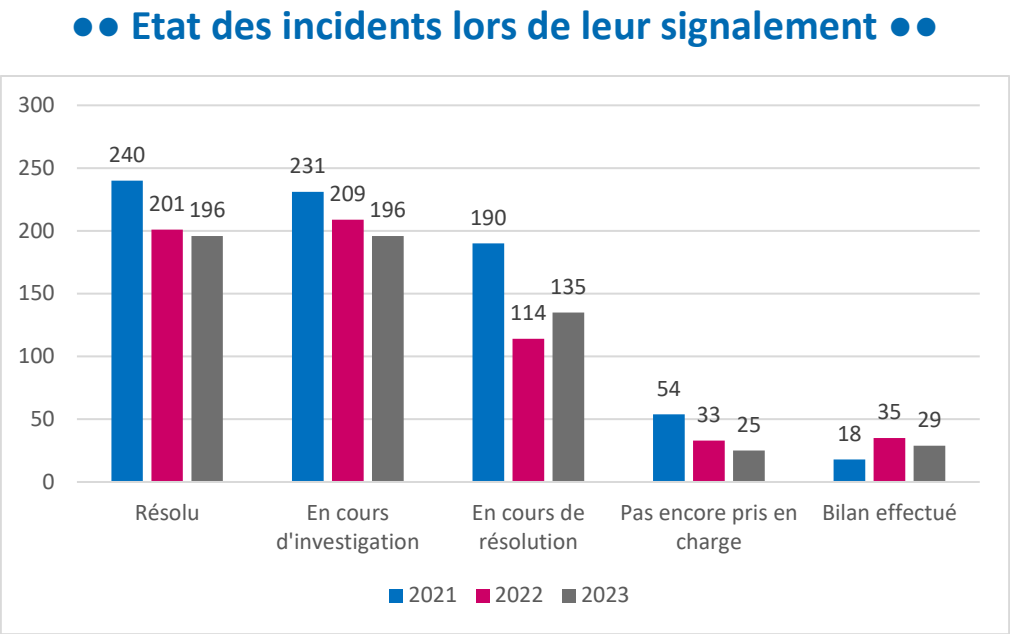

Figure 5 - Etat des incidents lors de leur signalement

En 2023, comme en 2022 et 2021, plus de la moitié des incidents sont résolus ou en cours de résolution par la structure avant leur déclaration. Le nombre d'incident pour lesquels le CERT Santé a été sollicité pour des actions d'investigation et d'aide à la remédiation a légèrement diminué cette année, pour atteindre **34% en 2023 au profit de d'incidents en cours de résolution par l'établissement.**

20 structures n'ont pas transmis d'informations complémentaires à la suite de leur déclaration, malgré une demande de compléments d'information et/ou une proposition d'appui**. 20% de ces incidents étaient potentiellement d'origine malveillante (compromission de boites de messagerie ou exploitation de vulnérabilités). Ce chiffre a presque doublé par rapport à 2022** (11).

29%

C'est le pourcentage de **signalements pour lesquels a été demandé un accompagnement en 2023**. Il est **identique à celui de 2022**.

Un accompagnement est demandé lors d'incidents ayant un impact important sur l'activité de la structure ou lorsqu'un évènement remonté par les équipements de sécurité du SI laisse présager une compromission potentielle. La structure veut s'assurer qu'elle a bien entrepris l'ensemble des actions recommandées tant en matière d'investigation que de remédiation. **La principale demande d'appui concerne la gestion des attaques virales et la compromission des systèmes**.

De nombreuses structures sollicitent le CERT Santé 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.

●● Répartition des signalements selon la localisation de la structure●●

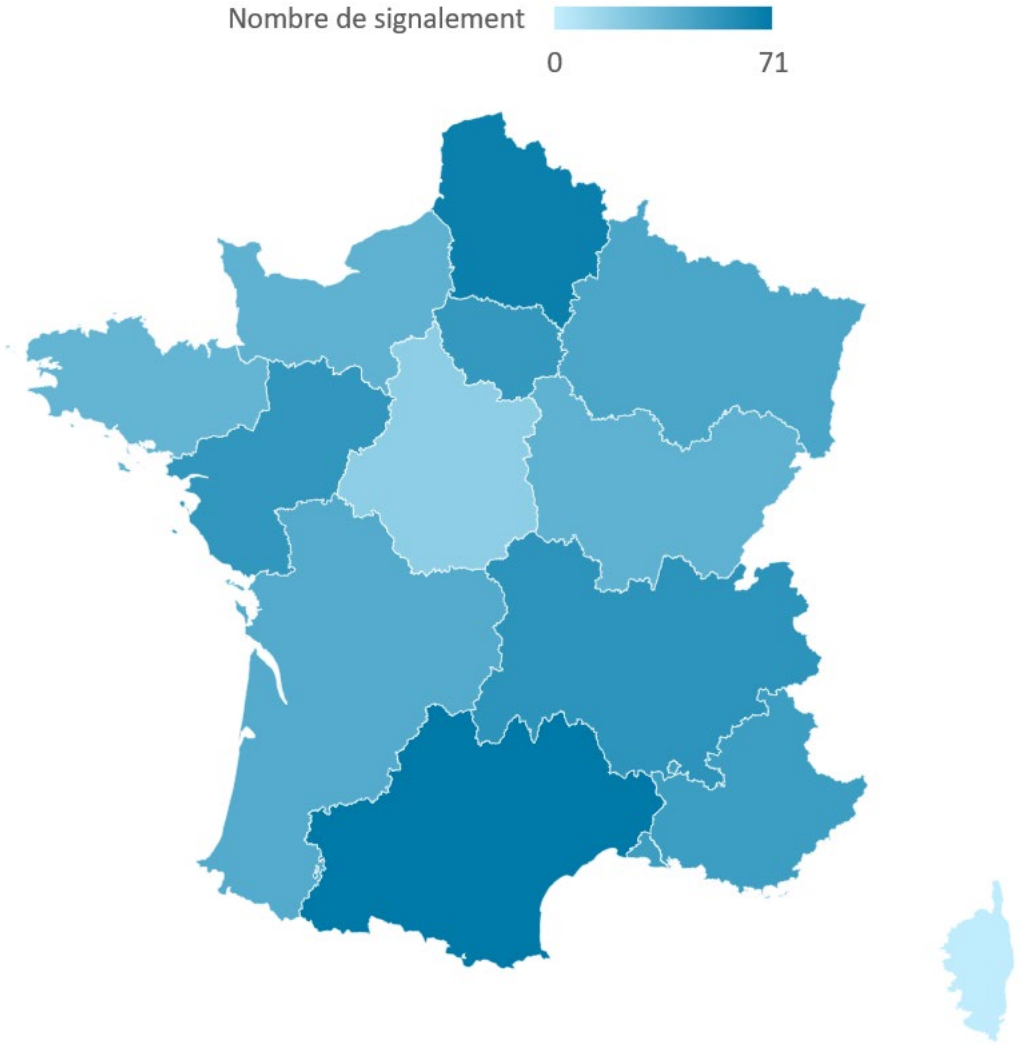

Figure 6 - Répartition des signalements par région

Les régions pour lesquelles le nombre de signalements est le plus important sont l'Occitanie (71), les Hauts-de-France (67) et l'Auvergne-Rhône-Alpes (55). Ces trois régions représentent à elles seules plus de 33% du total des signalements.

●● Nombre de signalements rapporté à l'activité hospitalière des régions ●●

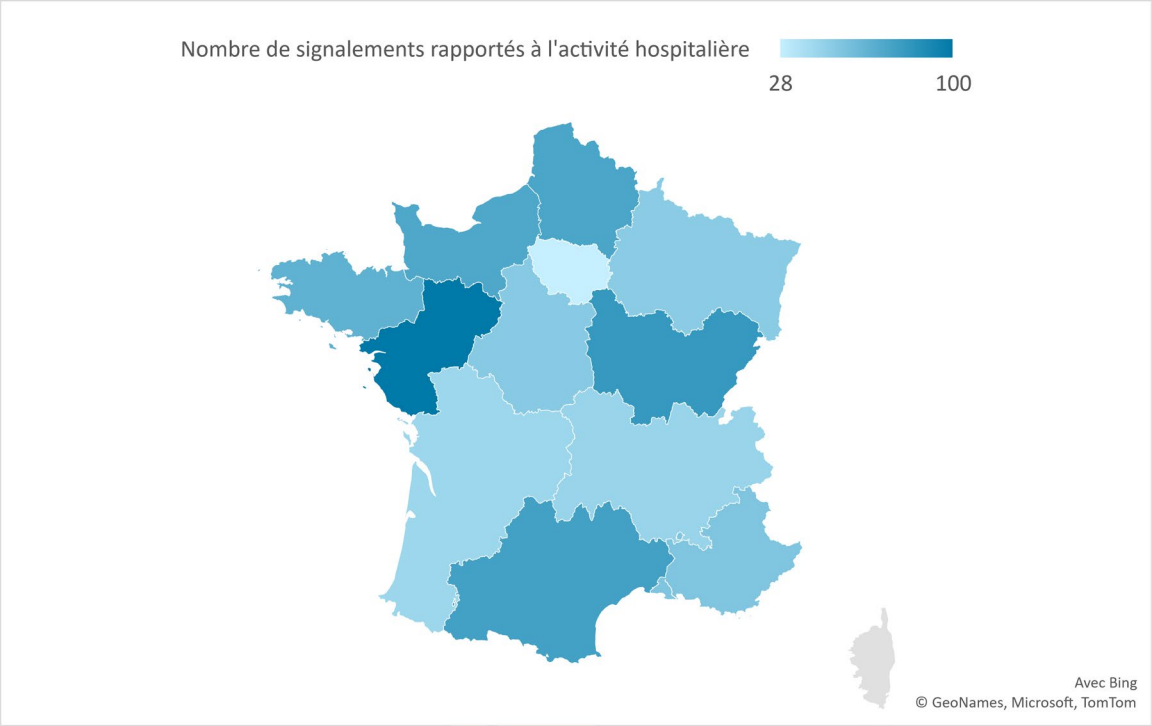

Figure 7 - Nombre de signalements rapporté à l'activité hospitalière des régions

Cette carte présente le ratio entre le nombre de signalements et l'activité hospitalière rapportée au niveau national[8] : plus une région a un nombre de signalements élevé par rapport à son activité, plus celle-ci est foncée. Les DROM-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 le ratio le plus élevé (Pays de la Loire) est utilisée en tant qu'indice 100.

Au regard de son activité hospitalière (5,1% de l'activité nationale), la région Pays de la Loire est en tête en matière de remontée des incidents. La région Bourgogne-Franche-Comté arrive en deuxième position. Les régions Occitanie, Hauts-de-France et Normandie arrivent en troisième position avec un ratio quasi-identique.

En revanche, la région Ile de France déclare peu d'incidents au regard du nombre d'établissements hospitaliers situés sur ce territoire de santé.

Il est nécessaire de rappeler à toutes les structures de santé l'obligation de déclaration des incidents de sécurité, en particulier dans les régions où le nombre de signalements rapporté à l'activité hospitalière est faible.

[8] INSTRUCTION N° DGOS/PF5/2019/32 du 12 février 2019 relative au lancement opérationnel du programme HOP'EN

Répartition des signalements selon le type de structure

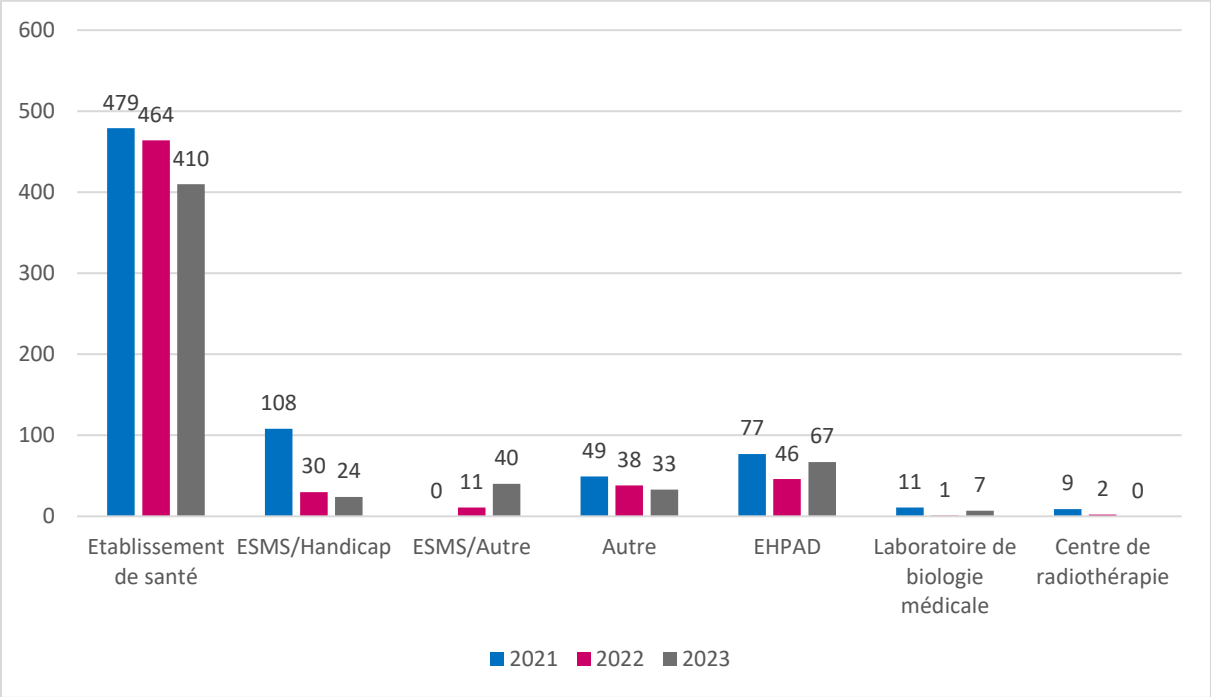

Figure 8- Répartition des signalements selon le type de structure

La grande majorité (71%) des incidents de sécurité est déclarée par les **établissements de santé** (voir détail figure 7).

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

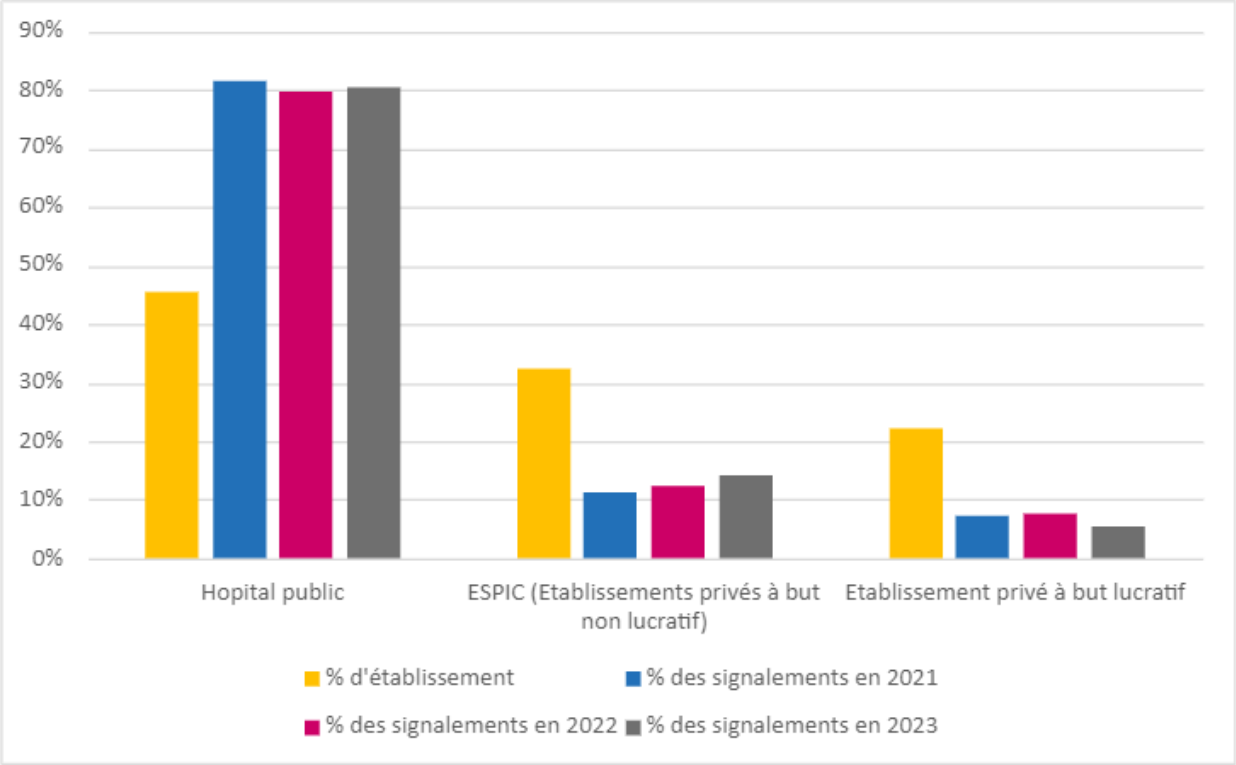

Figure 9 - Part des signalements comparée à la part des établissements selon leur raison sociale

Les parts des établissements dans la déclaration des incidents en 2023 est stable par rapport à 2022. **87 établissements référencés OSE** ont déclaré au moins un incident en 2023.

61 C'est le nombre de structures ayant déclaré plus de 2 incidents durant l'année 2023 sur 462 structures au total. Parmi elles, il y avait 301 établissements de santé et 121 établissements et services médico-sociaux. 8 établissements de santé ont signalé au moins quatre incidents.

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

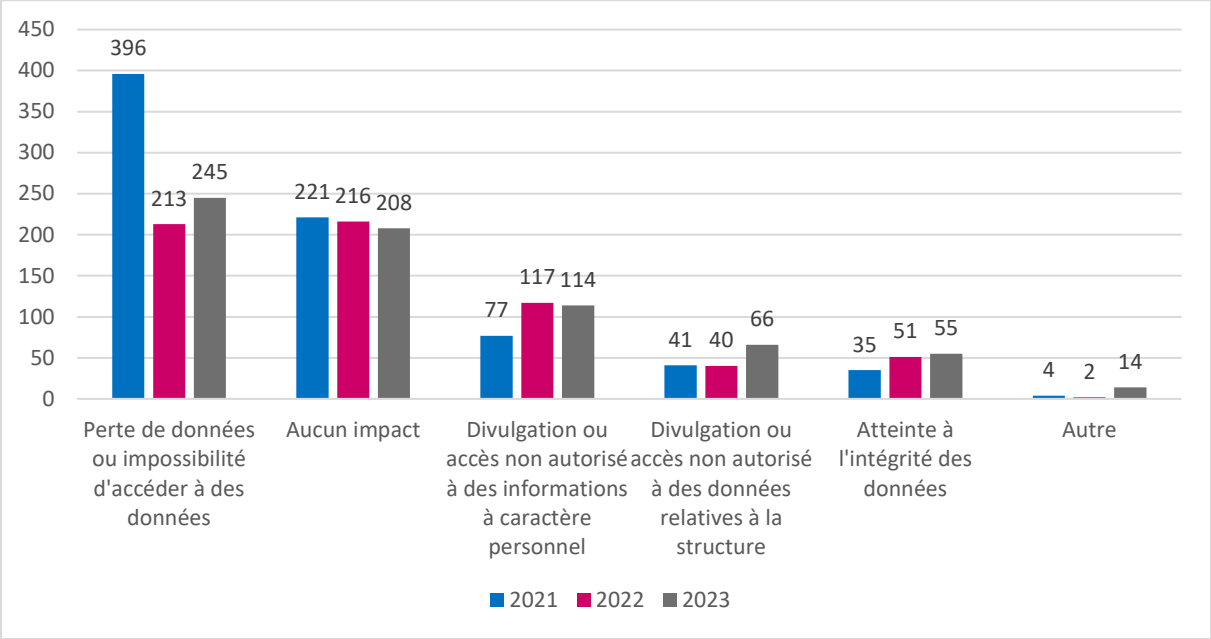

Figure 10- Répartition selon les types d'impact sur les données

En 2023, les incidents signalés où tout ou une partie des données des applications de la structure étaient devenues inaccessibles ont augmenté de 15% par rapport à 2022, principalement en raison d'incidents chez les hébergeurs (Hosteur, Coaxis), fournisseurs de DPI mais également des cas fréquents de coupures de liens télécoms (qui concernent souvent des incidents côté FAI).

Pour 30% des signalements, les structures assurent qu'il n'y a eu aucun impact sur les données. On retrouve alors des incidents ayant pour origine des tentatives d'hameçonnage ou d'intrusion sur le SI, des attaques par ingénierie sociale ou bien encore des bugs applicatifs ou une perte de la ligne téléphonique.

De plus, les cas de divulgation ou d'accès non autorisé à des informations à caractère personnel et données relatives à la structure est resté stable par rapport à l'année précédente. Parmi ces cas, la majorité implique le vol d'authentifiants par des pratiques telles que l'hameçonnage, le harponnage ou la recherche de mot de passe par force brute, entraînant une compromission des comptes de messagerie et Active Directory, souvent utilisés pour des campagnes d'hameçonnage ultérieures, des tentatives de latéralisation ou d'élévation de privilèges. On observe également une augmentation des cas de fuite d'informations suite à l'exploitation de vulnérabilités sur des équipements exposés sur Internet ou par exfiltration de données lors d'attaques par rançongiciel.

53% **C'est le pourcentage de structures indiquant que l'incident n'a eu aucun impact sur son fonctionnement en 2023. Ce chiffre est en baisse par rapport à 2022 mais présente une augmentation par rapport à 2021 puisqu'il était de 38%.**

32%

C'est le pourcentage de structures qui ont été contraintes de mettre en place en 2023 un **fonctionnement en mode dégradé** du système de prise en charge des patients (7% de moins qu'en 2022). 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 la période d'**une journée** mais certains établissements ont été confrontés à cette situation pendant plusieurs jours. **19**% des établissements ayant mis en place un mode dégradé ont subi une interruption du système de prise en charge d'un patient.

●● Répartition des déclarations selon le type de données impactées●●

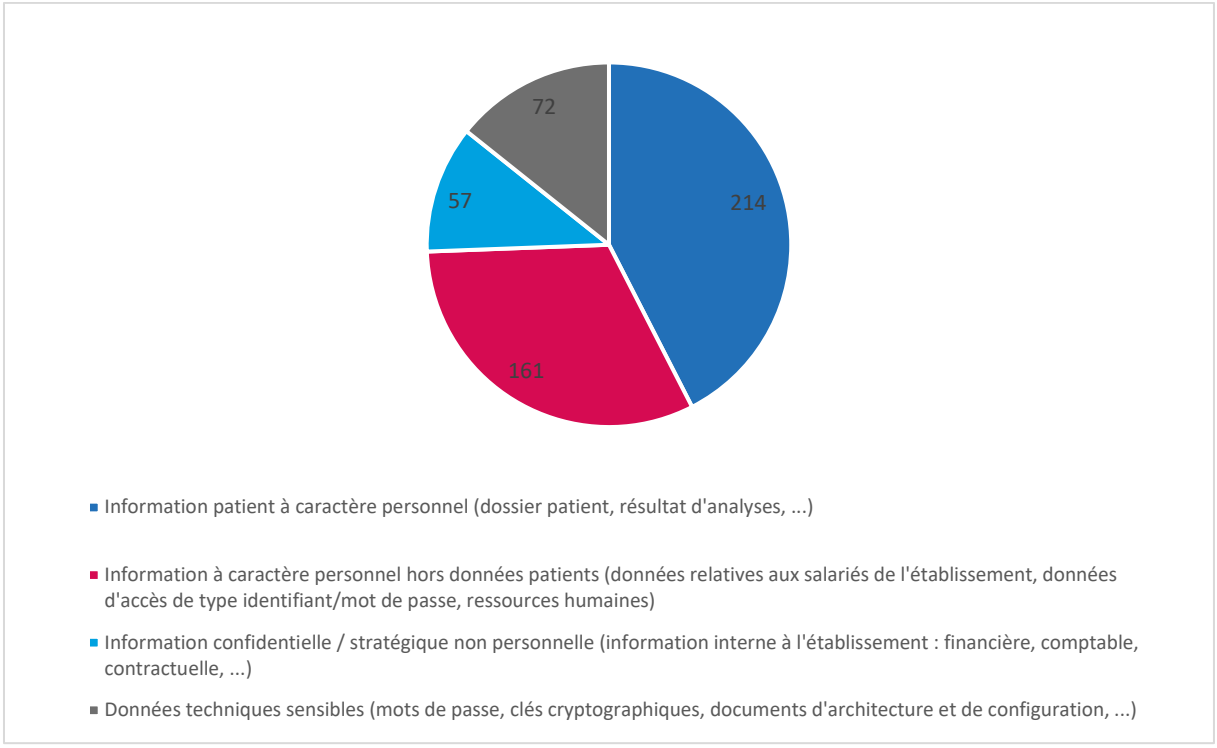

Figure 11 - Répartition selon les types de données impactées

59% C'est le pourcentage de structures indiquant que **l'incident a eu un impact sur des données**, qu'elles soient à caractère personnel, techniques ou relatives au fonctionnement de la structure.

24% des incidents impactant des données touchent **plus d'une catégorie de données** parmi les quatre catégories décrites dans le graphique ci-dessus.

C'est ainsi que parmi les incidents impactant des données, **42%** touchent des **données de santé à caractère personnel**, 32% des informations à caractère personnel hors données patient (principalement des identifiants de comptes utilisateur), 14% des données techniques sensibles et enfin 11% des informations confidentielles ou stratégiques. Les données à caractère personnel sont donc les premières atteintes par les incidents de sécurité déclarés.

●● Mise en danger potentielle des patients●●

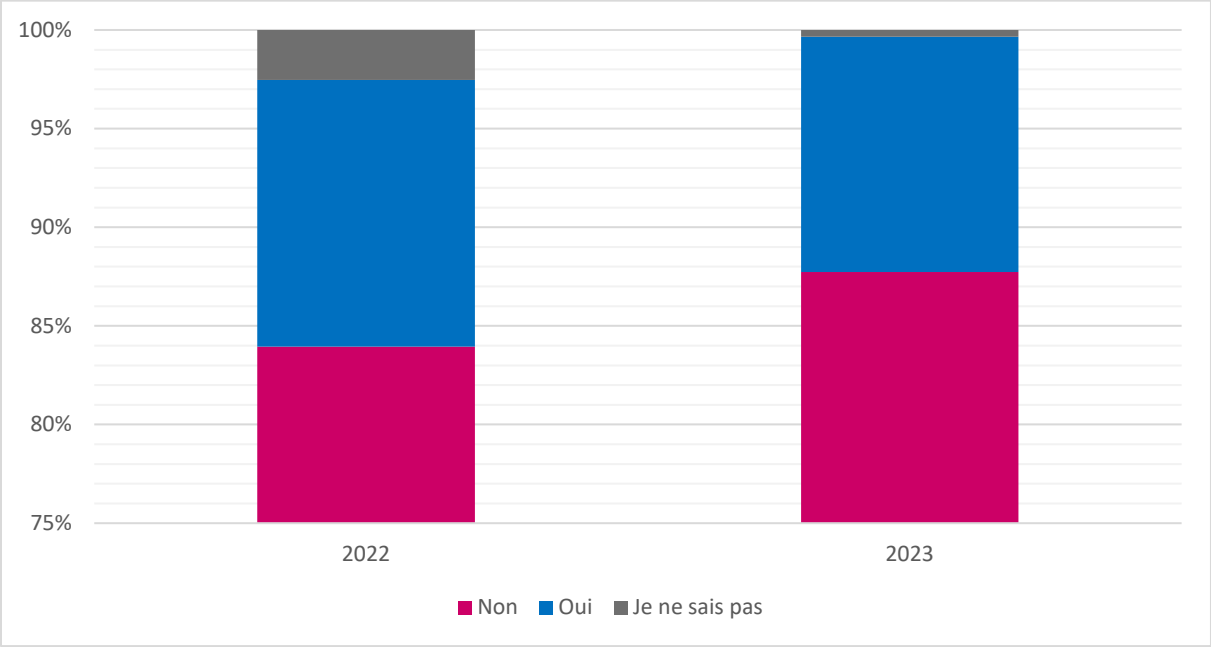

Figure 12 - Mise en danger potentielle des patients

Parmi les **69 mises en danger patient** de cette année 2023 (12% du nombre total d'incidents), **un seul incident a entrainé une mise en danger patient avérée**.

Les 68 incidents restants, correspondant à la part des mises en danger potentielles de patients, ont été attribués à diverses causes. Il s'agit notamment d'attaques par rançongiciel, de coupures de courant ou de liens télécom, ainsi que de pannes d'équipement. Ces incidents ont eu un impact direct sur la disponibilité des services de santé, entraînant des interruptions prolongées de l'accès à des services hébergés, des perturbations du service téléphonique du SAMU et des dysfonctionnements des logiciels de prescription/aide à la dispensation.

Ces situations ont engendré des risques plus ou moins accrus pour la sécurité des patients, mettant en évidence la nécessité de mesures préventives et d'une gestion proactive des incidents pour garantir la continuité des soins.

En outre, les dysfonctionnements des logiciels de prescription/aide à la dispensation, attribués à des bugs logiciels, ont été identifiés comme une cause supplémentaire d'incidents de mise en danger patient. Heureusement, la vigilance des professionnels de santé et la mise en place de procédures de détection d'erreurs ont contribué à limiter l'impact de ces incidents sur la sécurité des patients.

●● Répartition des signalements à origine malveillante ou non malveillante ●●

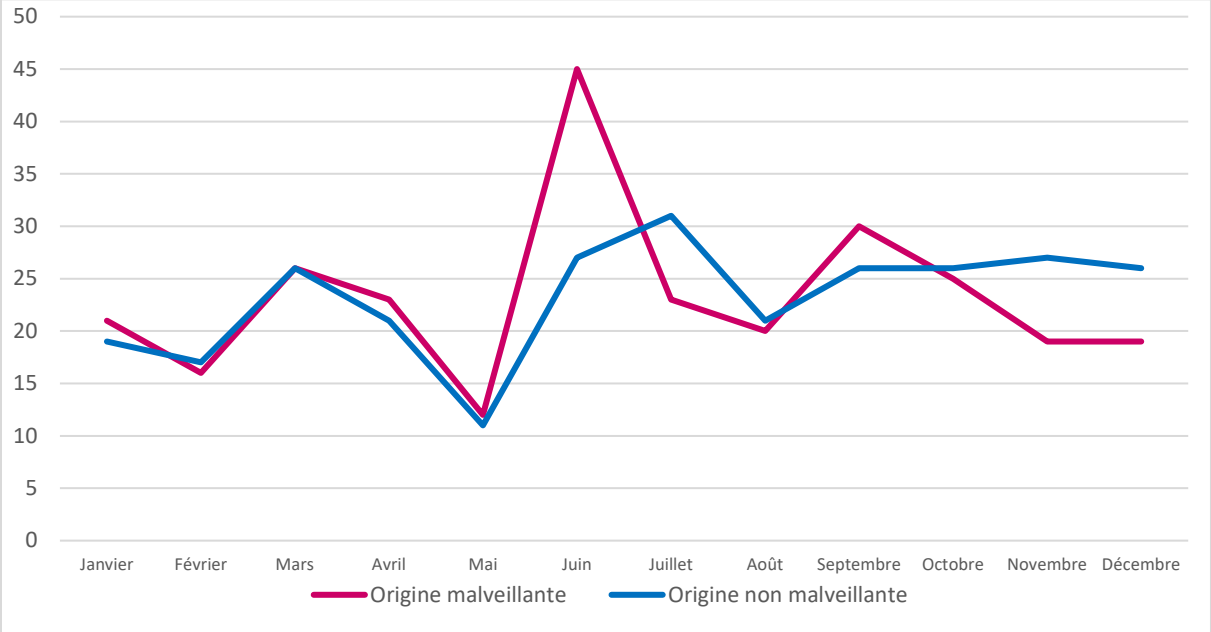

Figure 13 - Répartition selon le type d'incident

Parmi **les incidents déclarés, la moitié sont d'origine malveillante et l'autre moitié d'origine non malveillante**. Dans l'analyse détaillée de ces deux catégories d'incidents, sont exclus les 24 signalements dits « Hors périmètre » n'ayant pas fait l'objet d'un traitement particulier.

Les actes malveillants

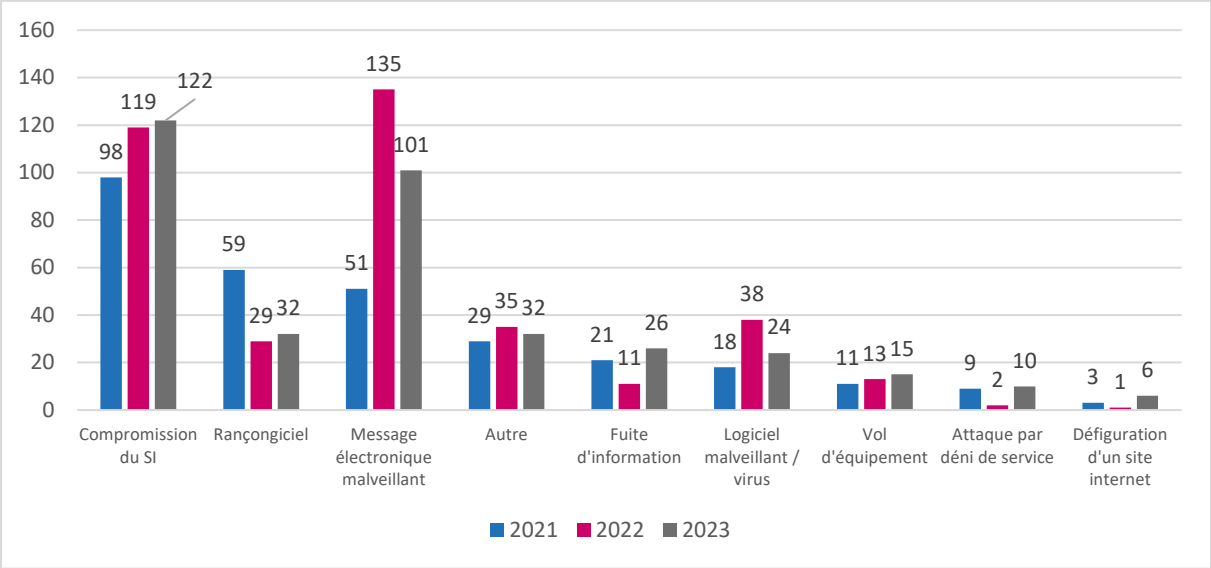

Figure 14 - Nombre d'incidents par type d'origine

L'année 2023 a été marquée comme en 2022 par une forte activité malveillante relative au vol d'identifiants (login – mot de passe) de comptes de messagerie et de comptes d'accès à distance. La baisse du nombre de signalements liés aux messages malveillants ne signifie pas une baisse de l'activité malveillante liée à l'hameçonnage ou aux malspam mais de celle des déclarations des activités malveillantes basées sur des campagnes n'ayant pas eu un réel impact sur les utilisateurs.

La compromission de comptes de maintenance des solutions d'infrastructures et applicatives des structures a également été observée cette année.

Les attaquants récupèrent les identifiants selon trois modes opératoires : la technique de l'hameçonnage (phishing), l'exploitation de vulnérabilités sur des équipements qui n'ont pas été mis à jour et les tentatives de récupération en testant un grand nombre de mots de passe (technique de brute force).

Les attaques par rançongiciel (32 au total) ont été équitablement réparties sur les 4 trimestres de l'année. Certaines d'entre elles ont causé des dysfonctionnements critiques au sein des établissements victimes à cause de la perte massive de données et ont été parfois précédées par une exfiltration d'informations confidentielles ou sensibles (en augmentation par rapport à 2022).

Il convient cependant de souligner l'impact significatif de l'intervention proactive du CERT Santé dans la prévention de l'exploitation de vulnérabilités permettant d'obtenir un premier accès au SI de la victime. Cela a concerné en particulier des accès VPN (Fortinet) ou des accès bureau à distance (Citrix Bleed) de plusieurs dizaines d'établissements.

Ainsi dans le cadre d'un accompagnement technique, plusieurs attaques ont été prises en charge dès leur phase initiale d'infiltration ou bien neutralisées avant la compromission de composants critiques du SI tels que l'Active Directory.

L'intervention rapide du CERT Santé suite aux signalements d'activités malveillantes en cours de réalisation sur le SI des victimes a permis de les neutraliser. Le CERT Santé a pu conseiller

la structure et ainsi stopper toute progression des attaques vers d'éventuelles étapes de chiffrement ou de propagation au sein du système d'information pouvant impacter plus largement l'Active Directory et des services numériques critiques.

Cette intervention proactive a permis de protéger les données critiques des établissements de santé, préservant ainsi l'intégrité et la continuité opérationnelle de leurs systèmes d'information.

En conséquence, ces actions ont évité des perturbations majeures pouvant compromettre le bon fonctionnement des systèmes d'information, voire les paralyser, ainsi que la nécessité de recourir à des solutions de récupération de données.

Il est rappelé la recommandation gouvernementale de ne jamais payer de rançon :

- Son paiement ne garantit pas l'obtention d'un moyen de déchiffrement, incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux ;
- Le paiement de la rançon n'empêchera pas l'entité d'être à nouveau la cible de cybercriminels ;
- L'expérience montre que l'obtention de la clé de déchiffrement ne permet pas toujours de reconstituer l'intégralité des fichiers chiffrés. En particulier, les fichiers modifiés par une application et chiffrés dans le même temps par le rançongiciel ont de fortes chances d'être corrompus (exemple : un fichier de base de données).
- Enfin, son versement s'apparente à subventionner une organisation criminelle.
- En outre, les sociétés assistant la victime dans le paiement de la rançon peuvent être poursuivies pénalement en France sur le fondement de la complicité d'atteinte au STAD et de Blanchiment.
- En cas de prise de contact avec les auteurs, il est fortement recommandé de le faire avec l'assistance d'un service de police spécialisé, qui dispose d'un cadre légal pour ce faire.

Les fuites d'information concernent des identifiants de connexion (principalement à des VPN, ou des comptes de messagerie) et des données de santé à caractère personnel.

La catégorie « Autre » concerne principalement des tentatives d'escroquerie par mail et par téléphone, des envois de clés USB contenant de la propagande et du contenu à caractère complotiste et des tentatives d'intrusion qui n'ont pas abouti.

Notons qu'une part des incidents (16%) relève de plusieurs qualifications. Par exemple, une attaque par rançongiciel, suite à la compromission d'un compte VPN lié à des identifiants en vente sur Internet relève des catégories suivantes : « fuite de données », « compromission de SI » et « rançongiciel ».

La catégorie « Logiciel malveillant / virus » correspond aux codes malveillants pouvant être utilisés pour exfiltrer des données, perturber le fonctionnement des machines, déployer des rançongiciels (QakBot démantelé en août 2023 opérant en tant qu'infostealer et associé à des activités de botnet) ou générer de la crypto-monnaie.

50% C'est le pourcentage des incidents qui ont une origine malveillante en 2023. Ce chiffre **est identique** à celui de 2022.

Observatoire des
(2023)

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

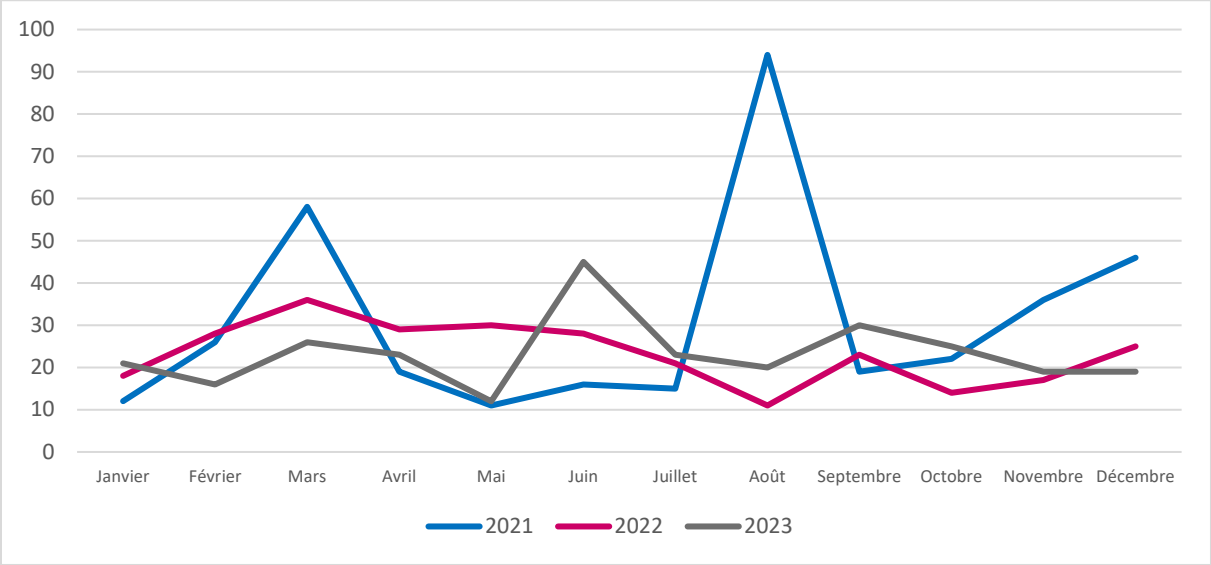

Figure 15 - Evolution du nombre d'incidents dont l'origine est malveillante

.

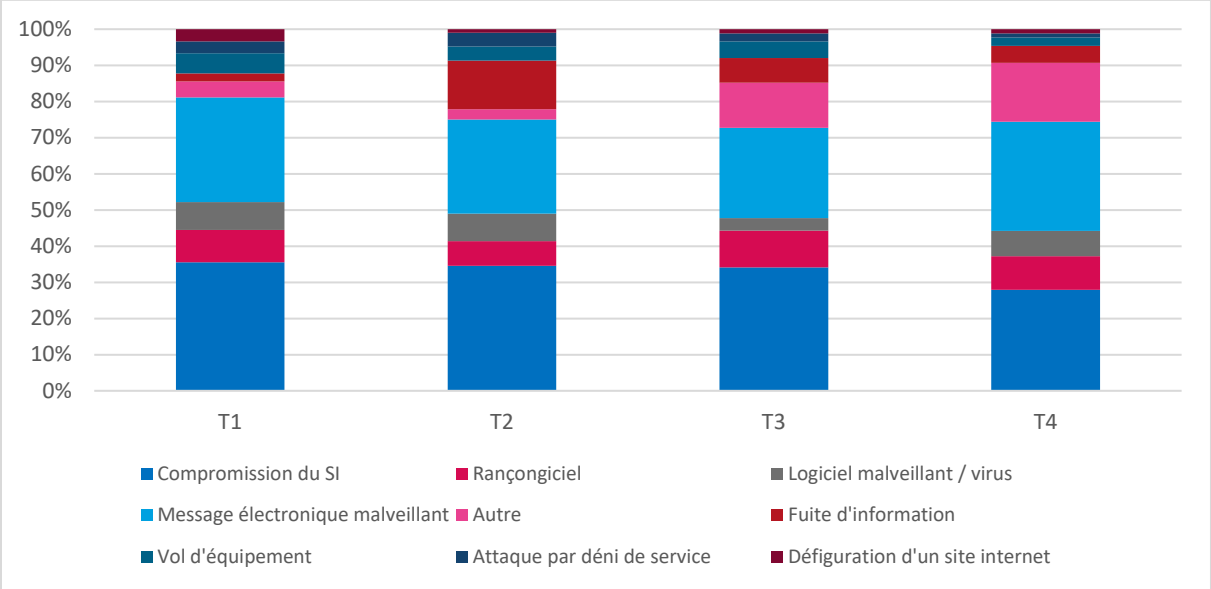

Figure 16 - Origine malveillante des incidents par trimestre

La frise chronologique suivante présente les rançongiciels et les principales vulnérabilités ayant fait l'objet d'une exploitation (mais sans lien avec les attaques par rançongiciel) et qui ont été identifiés au cours de l'année :

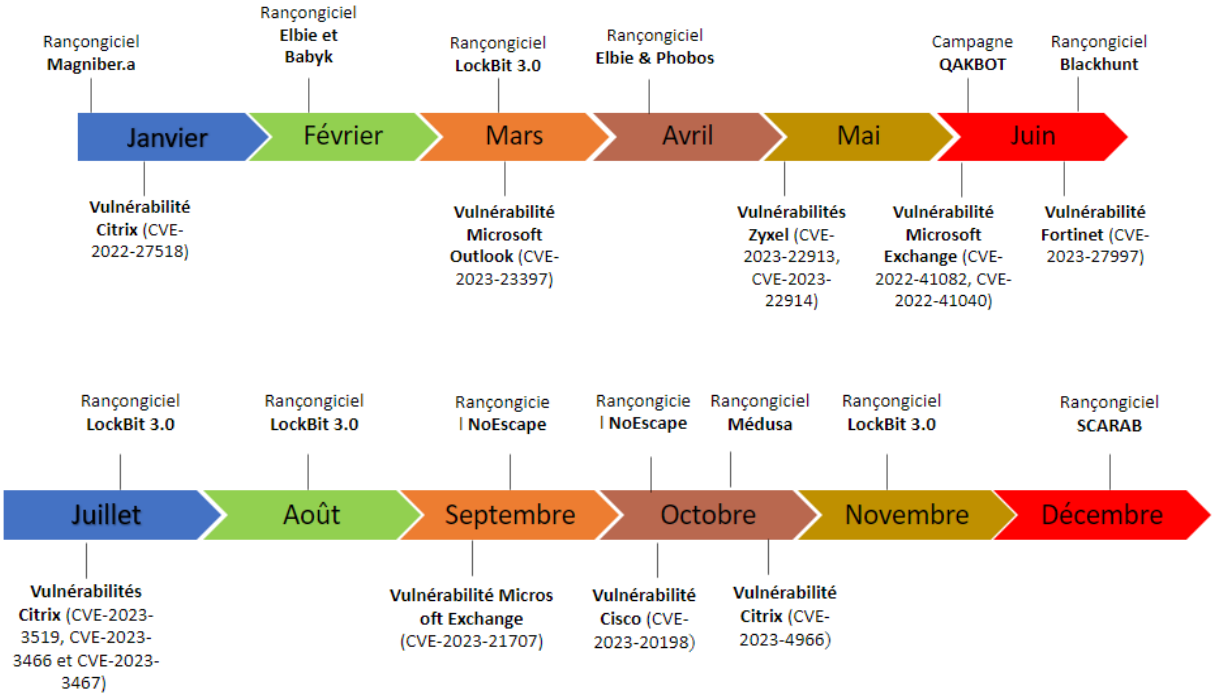

Figure 17 - Chronologie des cyber-menaces identifiées en 2023

●● Appui technique pour la résolution d'un incident ●●

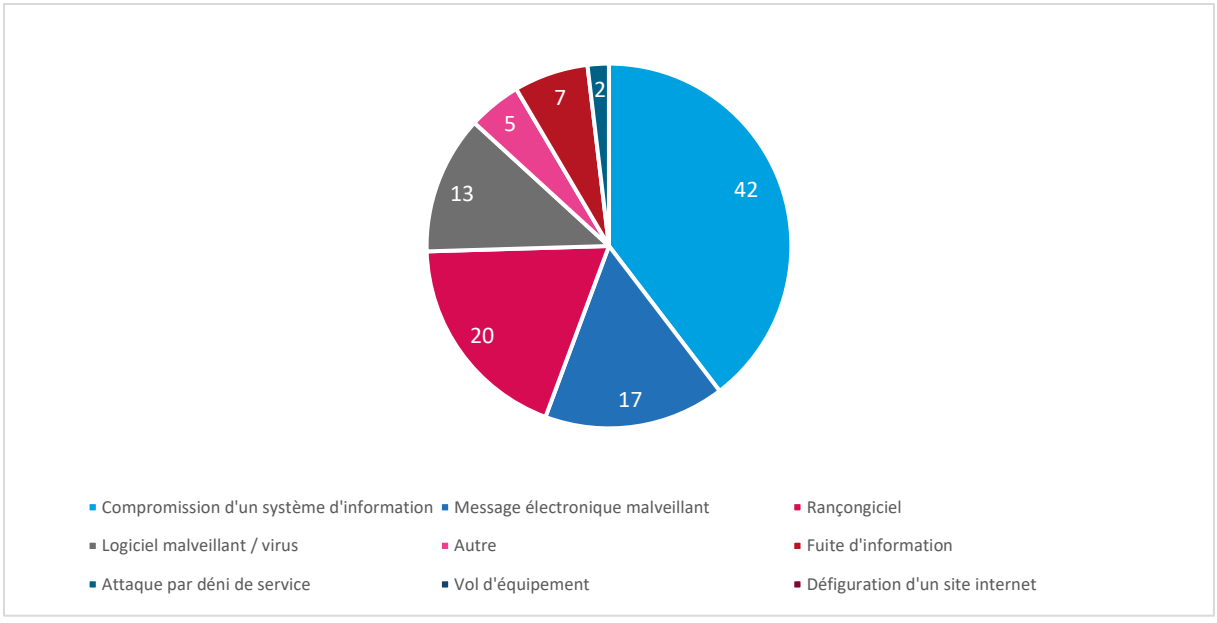

Figure 18 - Origine des incidents pour lesquels un appui technique a été apporté par le CERT Santé

Le nombre de déclarations d'incident pour lesquels une demande d'accompagnement est formulée est resté identique à l'année 2022. Il y a eu au total 165 demandes d'accompagnement, soit 28% des incidents traités. Elle concerne généralement une demande d'appui pour confiner des services compromis, identifier l'origine d'une compromission avérée ou potentielle du SI et la validation des mesures visant à endiguer la propagation de l'attaque et corriger les vulnérabilités. Ce sont les ES publics (49%) qui ont le plus sollicité le CERT Santé et en particulier les ES supports de GHT (24%).

Dans le cadre **de l'accompagnement des structures de santé**, des recommandations ont été émises par le CERT Santé afin, notamment, de permettre aux structures d'améliorer la sécurité de leur SI. Ces recommandations sont **adaptées à la taille de la structure ainsi qu'au niveau de technicité du déclarant et des équipes de la structure**.

Elles sont donc **variées** et peuvent aller de l'envoi des fiches et guides du portail cyberveille-santé, de la documentation de l'ANSSI, aux conseils plus techniques comme la mise en place de durcissement de systèmes, etc.

Les signalements d'origine non malveillante

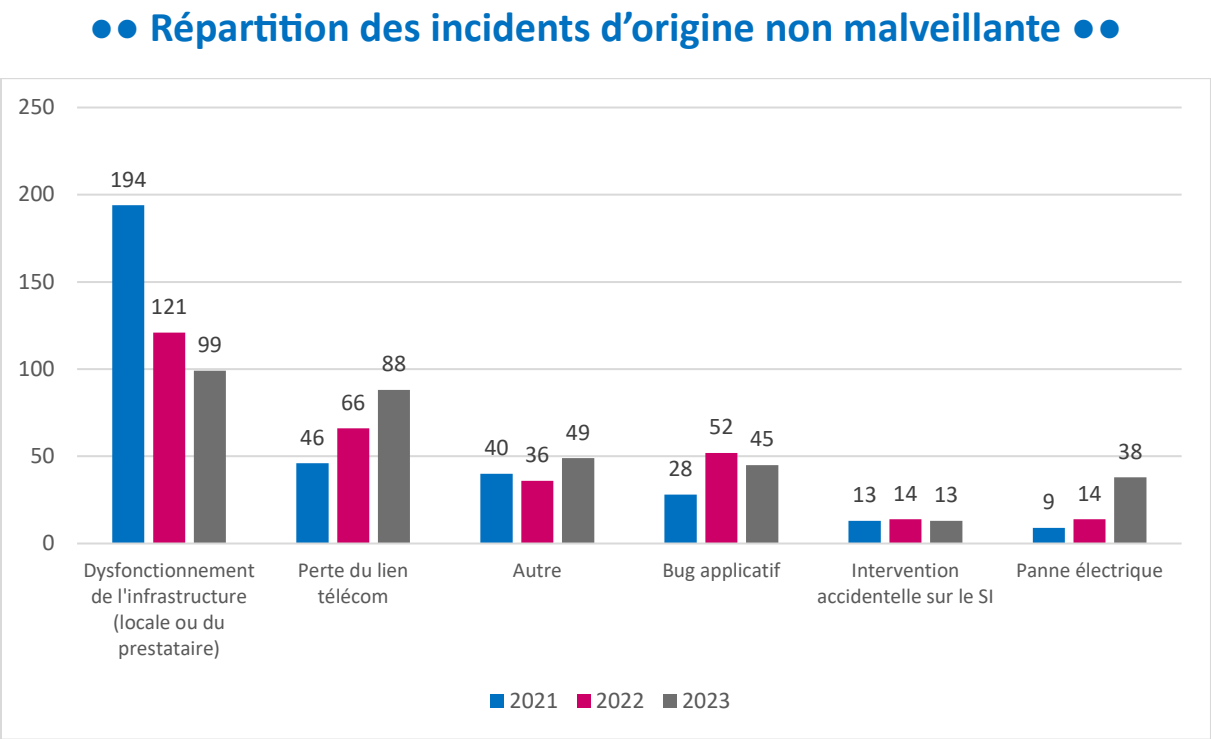

Figure 19 - Origine non malveillante des incidents

Le nombre d'incidents ayant une origine non malveillante est principalement lié à des mises à jour problématiques et des incidents issus des hébergeurs ou prestataires de solutions métier en mode SaaS. Cela a provoqué des interruptions prolongées de service ou des applications hébergées. **La part d'origine non malveillante et liée à un dysfonctionnement de l'infrastructure est de 35%**.

La **perte du lien télécom** est la deuxième source d'incident d'origine non malveillante (33%). Cette perte peut fortement impacter le fonctionnement des activités métier des structures de santé, en particulier les structures disposant d'un service d'urgences ou un SAMU. Ce type d'incident est généralement traité en priorité par les opérateurs.

Le nombre de déclarations lié à un **bug applicatif** (17%) est en diminution par rapport à 2022. Dans 40 % 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. Il arrive toutefois régulièrement que certains bugs applicatifs persistent dans le temps. Bien que ce cas reste minoritaire, voire marginal, il peut causer des désagréments aux établissements de santé dans leurs tâches quotidiennes. Dans de rares situations, le CERT Santé se positionne en tant qu'intermédiaire entre l'éditeur et l'établissement de santé, voire les potentielles parties prenantes qui pourraient avoir voix au chapitre, afin de faire avancer les choses et apporter un réel appui aux établissements de santé afin de réduire le temps d'indisponibilité de leurs outils.

Dans la catégorie « Autre » on retrouve principalement des déclarations de vulnérabilités qui n'ont pas fait l'objet d'une exploitation par un acteur malveillant mais également des

évènements informatiques à l'origine de comportements imprévus de systèmes mais qui se sont révélés être des « faux positifs » après une investigation du CERT Santé.

50% C'est la part d'incident d'origine non malveillante en 2023 des incidents, ce chiffre est constant par rapport à 2022.

Evolution des incidents d'origine non malveillante

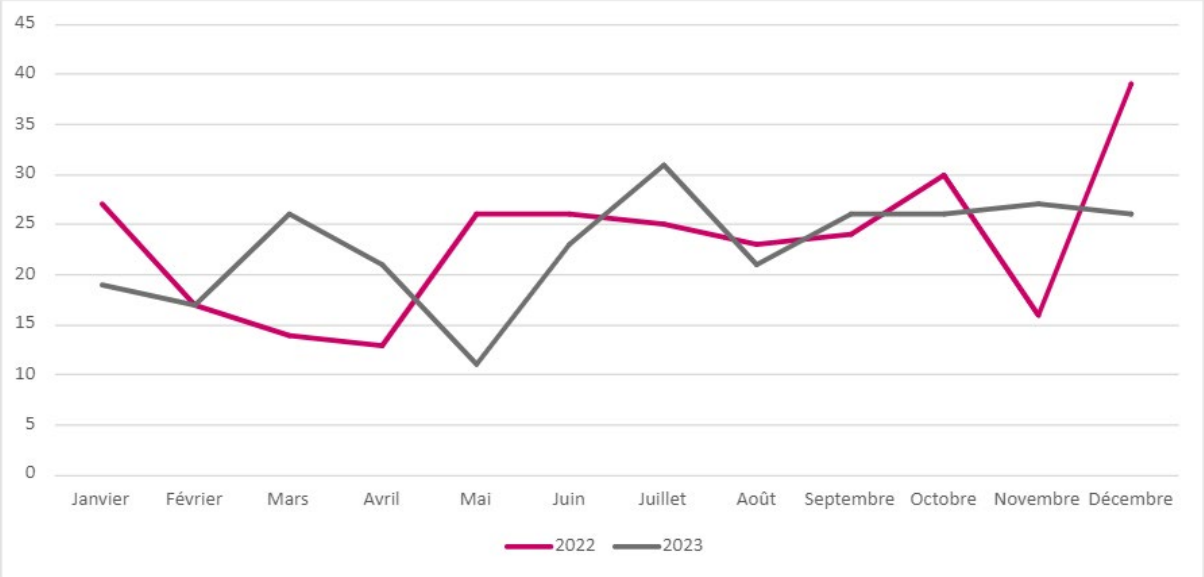

Figure 20 - Evolution du nombre d'incidents dont l'origine est non malveillante

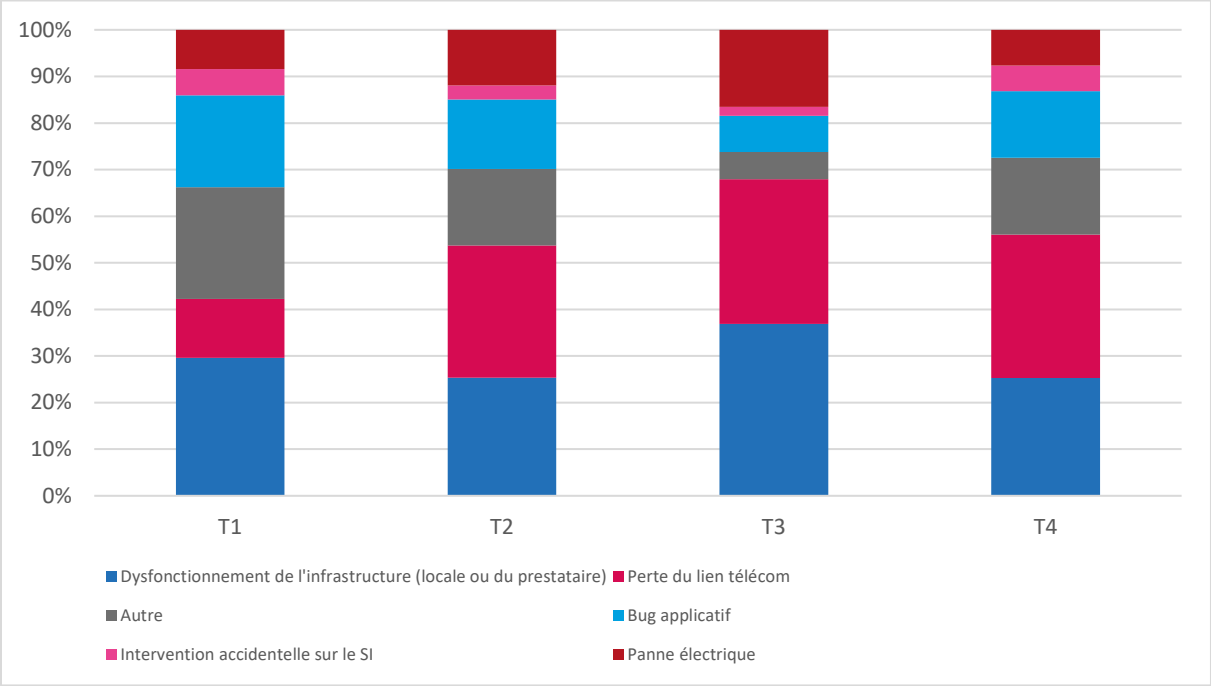

Figure 21 - Origine non malveillante des incidents par trimestre

4.3 Publication d'alertes sur le portail cyberveille-santé

En 2023,105 alertes ont été publiées sur le portail cyberveille-santé parmi lesquelles des

- Campagnes d'envoi de courriers alarmistes contenant une carte SD ou une clé USB (message à caractère complotiste) ;
- Campagnes de messages malveillants visant à conduite la victime à télécharger des binaires dangereux pour le poste et le reste du système d'information (Emotet, QakBot, Dridex, PikaBot).

Et

- Des vulnérabilités critiques activement exploitées concernant :
  - la solution d'accès à distance Citrix Netscaler ADC et qui permet à un attaquant non-authentifié de contourner l'authentification multi-facteur (Citrixbleed) ou d'exécuter du code arbitraire à distance ;
  - la messagerie Exchange et qui permet à un attaquant possédant un accès authentifié au serveur Exchange de pouvoir exécuter du code arbitraire à distance ;
  - la solution VPN Fortinet et qui permet à un attaquant non authentifié d'exécuter du code arbitraire ;

- la solution VPN Ivanti et qui permet à un attaquant non authentifié de créer un compte disposant de droits d'administrateur puis de téléverser des fichiers arbitraires sur le système afin d'exécuter du code arbitraire.

5 SERVICE NATIONAL CYBERSURVEILLANCE

Dans le cadre du plan de renforcement cyber du ministère, les audits de cybersurveillance ont été prioritairement orientés vers les groupements hospitaliers de territoire (GHT).

En 2023, 529 audits ont été réalisés : 432 CH sur 105 GHT (pour 72 GHT, plus de 50% des ES ont été audités), 77 établissements sanitaires, 18 ESMS et deux GRADeS.

6 VEILLE PROACTIVE

Le CERT Santé a renforcé son activité de veille proactive au regard du nombre important de vulnérabilités critiques qui ont fait l'objet d'une publication en 2023. Ainsi afin de prévenir la compromission potentielle ou avérée de SI au travers de l'exploitation de ces vulnérabilités, le CERT a alerté plus de 451 structures. Ces alertes ont principalement concerné des solutions d'accès à distance (VPN (Fortinet, Ivanti) ou bureau à distance (Citrix)) et l'environnement Windows (messagerie, suite Office).

Le CERT Santé a relayé près d'une centaine d'alertes concernant des compromissions avérées ou potentielles de SI identifiées par l'ANSSI.

7 CONSTAT ET RECOMMANDATIONS

Les structures qui ont été auditées ou alertées exposent souvent trop de ressources sur Internet et ne portent pas suffisamment d'attention à la sécurisation de leurs services (portail Web, accès à distance, etc…).

Les établissements de santé et médico-sociaux que le CERT Santé a accompagnés dans la réponse à incident présentaient parfois des faiblesses en matière de gestion des droits d'administration et de protection sauvegardes.

A partir d'octobre 2024, les établissements seront contraints d'élever leur niveau de sécurité dans le cadre de la mise en œuvre de la réglementation NIS 2. Une grande majorité d'entre eux seront concernés. Les exigences couvrent toutes les dimensions de la cybersécurité (organisationnelle et technique).

Le CERT Santé rappelle ci-dessous quelques bonnes pratiques afin d'améliorer la résilience des établissements vis-à-vis des menaces cyber les plus importantes comme les attaques par rançongiciel.

Maitriser les systèmes exposés

- Réduire la surface d'attaque en désactivant les comptes, protocoles et services qui ne sont pas indispensables : certaines structures de santé auditées exposent un grand nombre de services numériques sur Internet y compris des services de télé-administration reposant sur RDP ou d'autres protocoles.

- Renforcer les configurations et la sécurisation des accès : beaucoup de vulnérabilités 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 de configuration ;

- Vérifier la suppression des vulnérabilités web classiques (présentées dans le Top 10 OWASP9) : 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 vulnérabilités référencées par l'OWASP s'il est correctement configuré ;

- Mettre à jour les équipements (boitiers VPN, fermes RDS ou de virtualisation, routeurs d'interconnexion). Ils doivent faire l'objet d'une attention particulière et d'une réactivité adéquate face à la menace. En effet, des vulnérabilités critiques sont souvent utilisées par les attaquants pour se connecter sur un système d'information dans les quelques jours, voire quelques heures, après la publication d'une alerte. Il est nécessaire de se tenir informé des nouvelles vulnérabilités sur les équipements déployés, particulièrement les équipements exposés sur internet. Il en va de même pour les équipements constituant l'infrastructure interne, qui peuvent faciliter l'action d'un attaquant déjà infiltré sur le réseau privé.

[9] 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.

- Inclure un engagement du prestataire (DPI, Gestion des activités de biologie médicales, gestion des activités de radiologie, etc…) sur le maintien en conditions de sécurité de son infrastructure : 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 conditions de sécurité ainsi que la possibilité de réaliser des audits.

Le premier appel à financement (« Domaine 1 ») du programme CaRE pour les établissements de santé vise le renforcement de leur niveau de sécurité en maitrisant leur exposition. Le scan réalisé tous les deux mois doit permettre de maintenir une surveillance continue et de s'assurer de l'absence de vulnérabilité critique.[10]

Mettre en place de l'authentification double facteur sur les applicatifs exposés et critiques :

La récupération des mots de passe par force brute, le phishing et à l'infostealing est grandissante. Le CERT Santé constate de plus en plus que des attaquants accèdent initialement aux systèmes avec des identifiants valides récupérés par les méthodes précitées dans les cas de compromissions, principalement sur les passerelles VPN et applicatifs exposés.

- Activer l'authentification multifacteur basée sur le temps (mot de passe changeant toutes les X secondes, nommé TOTP). Ainsi pour accéder au système, l'attaquant devrait en plus de posséder le couple identifiant / mot de passe valide, posséder ce second facteur d'authentification. Le multifacteur par mail est un compromis qui ne couvre pas correctement le risque de vol d'identifiants, les utilisateurs ayant souvent les mêmes identifiants pour leur boîte mail.

Le référentiel sur l'identification électronique définit des exigences sur les connexions à des services numériques traitant des données de santé (mots de passe robustes, authentification multi-facteurs et utilisation d'informations d'identification des utilisateurs vérifiées et issues des répertoires de référence (INS, RPPS, FINESS). Il décrit des paliers successifs à atteindre, entre le 1er juin 2022 et le 31 décembre 2025. Il est opposable et le respect des exigences correspondantes est obligatoire pour les acteurs concernés.[11] Dans ce contexte, l'objectif de l'appel à projet HospiConnect est d'accélérer le déploiement des exigences du référentiel d'identification électronique et de réduire les risques d'usurpation de l'identité numérique des professionnels de santé pour l'accès aux services sensibles. Il est intégré au Programme CaRE dans le cadre de l'axe 4 "Sécurité opérationnelle".

[10] https://esante.gouv.fr/strategie-nationale/cybersecurite#content-38127

[11] https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

Sécuriser ses sauvegardes

Dans de nombreux incidents liés à une attaque par rançongiciel, les ES n'ont pas pu exploiter les sauvegardes qui étaient chiffrées. Ainsi, la présence de sauvegardes intègres aurait permis de diminuer sensiblement le temps de reprise d'activité.

- Identifier les données critiques et réaliser des sauvegardes automatiques et récurrentes, si possible de façon sécurisée (chiffrement des sauvegardes) ;
- s'assurer de la restriction d'accès aux sauvegardes en :
  - privilégiant un accès avec un compte d'administrateur local avec une authentification à deux facteurs, ce compte n'étant pas référencé dans l'Active Directory ;
  - restreignant l'accès aux composants d'administration aux seules adresses IP des rebonds ou postes autorisés (que cela soit l'interface d'administration de la sauvegarde ou l'administration du serveur qui l'héberge) ;
  - veillant à ce que l'utilisateur qui lance l'agent de sauvegarde sur les différentes machines n'a pas d'accès sur l'interface d'administration de l'application de sauvegarde ni de droits de suppression/modification des anciennes sauvegardes.
- veiller à ce que les outils liés à la sauvegarde soient à jour avec les derniers patchs de sécurité.

Le deuxième appel à financement (« Domaine 2 ») du programme CaRE pour les établissements de santé vise le renforcement de la stratégie de continuité et de reprise d'activité. Il intègre des exigences liées à la gestion des sauvegarde (architecture, supervision, immuabilité, authentification, etc.…) et à leur restauration en cas de crise, en particulier concernant les AD.

Se préparer à un incident cyber

- Organiser des exercices de gestion de crise cybersécurité[12] proches des conditions réelles afin de s'approprier des automatismes et d'assurer au mieux la continuité des soins en cas d'incident
- Réaliser des plans de continuité et de reprise d'activité
- Réaliser régulièrement des tests de restauration de ses sauvegardes afin de disposer de sauvegardes opérationnelles. Il est recommandé de consigner les résultats de ces tests dans un document unique de suivi dans lequel se trouvera : le statut des restaurations, la réévaluation éventuelle du périmètre critique à sauvegarder et le statut sur les risques identifiés. Pour la réplication, nous vous préconisons la sauvegarde en système 3-2-1 .

Maintenir la cartographie de son SI à jour

- Créer, maintenir ou mettre à jour une cartographie du système d'information

Cette cartographie référence l'architecture réseau, les flux de sécurité, la liste la plus exhaustive possible des applicatifs et leurs versions déployées. Cette cartographie permet de

[12] https://esante.gouv.fr/strategie-nationale/cybersecurite

réagir plus rapidement pour isoler des parties du réseau en cas d'attaque ou de participer au diagnostic lors de dysfonctionnements quel que soit leur origine.

Gestion des comptes

Les règles de gestion de mot de passe définies par l'ANSSI ou la CNIL ne sont toujours pas appliquées (politiques de mot de passes trop simples (6 à 8 caractères) acceptant les mots courants, les motifs prévisibles et des informations personnelles publiques).

- Avoir un mot de passe de 12 caractères, avec lettres (majuscules et minuscules), chiffres, caractères spéciaux pour les utilisateurs non privilégiés. Lorsque ces règles sont appliquées, il n'est pas nécessaire d'imposer l'expiration du mot de passe pour les comptes utilisateurs de l'Active Directory.
- Avoir un mot de passe de 16 caractères, avec lettres (majuscules et minuscules), chiffres, caractères spéciaux pour les administrateurs avec un renouvellement obligatoire tous les 1 à 3 ans (sauf connaissance de fuite).
- Utiliser un gestionnaire de mots de passe. C'est obligatoire pour la population des administrateurs et recommandé pour les utilisateurs. La non-connaissance d'autre mot de passe que le mot de passe maître du coffre-fort est un réel atout pour la sécurité du SI.

Pour en savoir plus, nous vous recommandons la lecture de la partie «4 - Facteur de connaissance » du guide de l'ANSSI : Recommandations relatives à l'authentification multifacteur et aux mots de passe.

L'annuaire Active Directory (AD) est un élément critique permettant la gestion centralisée de l'ensemble des permissions sur les différents domaines qui composent un système d'information (SI) Microsoft. L'obtention de privilèges élevés sur l'AD entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI. Il est donc primordial de réaliser un cloisonnement logique des ressources de l'AD pour réduire ce risque. Une des dimensions de ce cloisonnement est la restriction de l'utilisation de comptes à privilège et des différents niveaux d'administration proposés par cette technologie. Le Domaine 1 du programme CaRE vise à atteindre un premier niveau de remédiation suite à la mise en œuvre bimestrielle d'un audit ADS de l'ANSSI[13].

Savoir être réactif :

- Systèmes exposés, systèmes critiques, les vulnérabilités sont exploitées sous quelques jours voire heures ;
- Importance d'avoir la capacité de mettre à jour ces systèmes dans des délais très courts : équipes, procédures, etc. Voire de savoir déconnecter certains systèmes temporairement en maitrisant les impacts (cf VPN, etc) :

[13] https://esante.gouv.fr/strategie-nationale/cybersecurite#content-38127

- Importance aussi de suivre les alertes CERT, i.e. disposer en établissement d'un point de contact qui relève très régulièrement la boite déclarée (cela a déjà permis d'arrêter des attaques après le premier niveau de compromission).

Mettre en place un système de journaux centralisé

Lors d'attaques, les journaux d'évènements sont un bon moyen pour comprendre ce qu'il s'est passé. Mais la journalisation est surtout importante pour permettre de détecter dès les premiers signaux d'une attaque en cours, les traces liées aux actions des attaquants.

- Centraliser des journaux de logs de qualité et remonter des alertes automatiques basées sur des évènements anormaux (scan réseau / tentatives de force brute / désactivation d'antivirus …) peut être un réel atout pour détecter et endiguer une attaque en cours.

- Analyser régulièrement les journaux de ses équipements périmétriques : installer un correctif pour une vulnérabilité critique sur un composant exposé sur Internet n'est pas la garantie d'être protégé contre une exploitation antérieure, il faut également analyser ses journaux pour vérifier si elle a été exploitée et en cas de doute renouveler l'ensemble de ses comptes.

8 GLOSSAIRE

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
CERT	Computer Emergency Response Team
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
Forensique	L'analyse forensique en informatique signifie l'analyse d'un système informatique après avoir été victime d'une cyberattaque.
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 chargé de la Santé : sante.gouv.fr
- le site de l'Agence du Numérique en Santé : esante.gouv.fr
- le portail du CERT Santé : cyberveille-sante.gouv.fr/

Pour prendre contact :

- au sein du Ministère chargé de la Santé :

  ssi@sg.social.gouv.fr

  au sein de l'Agence du Numérique en Santé (CERT Santé) :
- cyberveille@esante.gouv.fr

MINISTÈRE
DU TRAVAIL
DE LA SANTÉ
ET DES SOLIDARITÉS
Liberté
Égalité
Fraternité

HFDS
HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici