RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date : 7 novembre 2024
Version : 1.0
Nombre de pages : 45

SECTEUR DE LA SANTÉ

ÉTAT DE LA MENACE INFORMATIQUE

TLP:CLEAR

Table des matières

1 SYNTHÈSE

Le secteur de la santé est un secteur hautement critique. Les incidents d'origine informatique qui l'affectent peuvent engendrer des conséquences significatives en termes de disponibilité, d'intégrité, de confidentialité et de traçabilité pour les services fournis et les données hébergées, pouvant aller jusqu'à la mise en danger de la vie humaine.

Il se compose d'un ensemble d'acteurs caractérisés par leur fragmentation et leur hétérogénéité. Cet état de la menace en distingue plusieurs catégories, allant des acteurs liés à la gestion du système de santé, aux prestataires de soins, en passant par les industriels de produits de santé et les fournisseurs et prestataires pour le secteur de la santé. Les patients ne sont toutefois pas inclus dans le périmètre du document.

L'ensemble de ces caractéristiques fait de ce secteur une cible de choix pour les acteurs de la menace, qu'ils proviennent de la sphère cybercriminelle, hacktiviste ou qu'ils soient soutenus par des États.

Les acteurs composant le secteur de la santé sont ainsi davantage ciblés de façon opportuniste par des attaques informatiques à but lucratif pouvant s'appuyer sur le déploiement de rançongiciels, l'exfiltration et la revente de données personnelles ou de santé, ou l'emploi de diverses techniques de fraude comme le recours à des faux sites web, l'usurpation de marque et la compromission de systèmes informatiques pour escroquer ou détourner des sommes d'argent.

Dans une moindre mesure, les acteurs du secteur de la santé sont également la cible d'attaques à finalité d'espionnage, liées notamment à des modes opératoires d'attaques (MOA) réputés associés à des États comme la Russie, la Chine, l'Iran ou la Corée du Nord. Dans le contexte de la pandémie de Covid-19, plusieurs MOA réputés étatiques ont notamment été utilisés pour cibler des données liées aux recherches sur la Covid-19, sur les vaccins et traitements développés ou encore sur les stratégies sanitaires nationales mises en œuvre.

Les acteurs du secteur de la santé peuvent également être la cible d'attaques à visée déstabilisatrice. Ces dernières prennent le plus souvent la forme d'attaque par déni de service distribué (DDoS), de défigurations de sites web, d'exfiltrations de données à des fins de divulgation ou encore d'attaques informatiques à visée de sabotage, et sont généralement conduites par des groupes hacktivistes en réaction à l'actualité.

Cet état de la menace portant sur le secteur de la santé comprend par ailleurs un volet dédié aux recommandations de l'ANSSI, qui sont destinées à éclairer les entités évoquées en matière de bonnes pratiques de cybersécurité à adopter afin de se prémunir contre les menaces abordées. Ces recommandations ne sont pas exhaustives, ne se substituent pas aux réglementations spécifiques qui peuvent concerner certaines entités, et doivent être adaptées et complétées dans le cadre du contexte opérationnel et fonctionnel du système d'information considéré.

Il est pleinement intégré aux initiatives engagées par l'ANSSI, le ministère de la santé et l'ensemble des parties prenantes (ANS, ARS, GRADeS, fédérations, etc.) en faveur du renforcement de la sécurité informatique du secteur et qui commencent à porter leurs fruits.

2 AVANT-PROPOS

2.1 Méthodologie

Ce document est un état de la menace informatique portant sur le secteur de la santé. Il présente les éléments de tendance permettant de comprendre la nature et les évolutions de la menace depuis l'année 2020, marquée par le début de la crise sanitaire liée à la Covid-19, jusqu'à l'année 2024. Il s'appuie sur l'analyse d'incidents rapportés à l'ANSSI et des éléments disponibles en source ouverte.

Il s'intéresse notamment aux catégories d'acteurs suivantes :

- les acteurs liés à la gestion du système de santé ;
- les prestataires de soins ;
- les industriels de produits de santé ;
- les fournisseurs et prestataires pour le secteur de la santé.

Les patients ne sont pas inclus dans le périmètre de cet état de la menace.

2.2 Le cadre législatif français et européen relatif au secteur de la santé sur le plan numérique

Du fait de la criticité du secteur de la santé, les entités qui le composent sont soumises à un cadre législatif variant en fonction de leur nature et de leurs activités, parmi lequel et de façon non exhaustive, les règlementations qui suivent.

Textes non-spécifiques au secteur de la santé[1] **:**

- le Règlement Général sur la Protection des Données (RGPD) ou règlement (UE) 2016/679 ;
- la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- les directives européennes « Sécurité des réseaux et de l'information » (*Network and Information Systems* ou NIS) 1 et 2 ;
- la directive européenne sur la Résilience des Entités Critiques (REC) ;
- le règlement européen sur la cyberrésilience (*Cyber Resilience Act* ou CRA) ;
- le dispositif national de Sécurité des Activités d'Importance Vitale (SAIV) ;
- les dispositions cyber des Lois de Programmation Militaire (LPM).

Textes spécifiques au secteur de la santé :

- des règlements européens portant sur les dispositifs médicaux (2017/745/UE) et les dispositifs médicaux *in vitro* (2017/746/UE) qui comportent une partie cyber ;
- le règlement européen relatif à l'espace européen des données de santé (European Health Data Space ou EHDS) ;
- le Code de la Santé Publique et notamment ses articles relatifs à la mise à disposition des données de santé (L1460-1 à L1462-2), aux services numériques en santé (L1470-1 à L1470-6), à l'hébergement des données de santé (L1111-8) et à la démarche de signalement des incidents de sécurité des systèmes d'information de santé (L1111-8-2).

1. La directive NIS 2 et la directive sur la Résilience des Entités Critiques (REC) ont été transposées dans le droit français en octobre 2024 à travers le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. Ce projet de loi doit être examiné par le Parlement avant son adoption.

2.3 Les principaux acteurs du secteur de la santé

Le périmètre du secteur de la santé tel que défini dans cet état de la menace s'organise autour de quatre catégories d'acteurs.

2.3.1 Les acteurs liés à la gestion du système de santé

Les acteurs liés à la gestion du système de santé occupent un rôle stratégique dans le pilotage, le financement et le contrôle du système de santé.

Types d'acteurs liés à la gestion du système de santé en France :

- le ministère de la Santé et de l'accès aux soins et le ministère des Solidarités, de l'Autonomie et de l'Égalité entre les femmes et les hommes ainsi que les établissements nationaux qui en dépendent tels que les caisses nationales, les agences sanitaires, l'Agence du Numérique en Santé (ANS) ;
- les acteurs régionaux tels que les agences régionales de santé (ARS), les caisses primaires d'assurance maladie ou encore les groupements régionaux d'appui au développement de la e-santé (GRADeS) ;
- les organismes représentant les différents acteurs du système de santé tels que les ordres professionnels, les syndicats professionnels, les fédérations professionnelles, etc ;
- les organismes offrant des complémentaires santé.

2.3.2 Les prestataires de soins

Les acteurs liés à la prestation de soins sont en contact direct avec des patients dans le cadre du parcours de soin : prévention, diagnostic, traitement, post-traitement, surveillance et accompagnement.

Types d'acteurs liés à la fourniture de soins en France :

- les établissements de santé publics, privés d'intérêt collectif et privés à but lucratif ;
- les établissements médico-sociaux ;
- les structures d'urgence ;
- les professionnels de santé libéraux ;
- les pharmacies d'officine ;
- les laboratoires d'analyse médicale ;
- les centres d'imagerie.

2.3.3 Les industriels de produits de santé

Les industriels de produits de santé désignent l'ensemble des acteurs en charge de la conception, la fabrication, la distribution et la vente de médicaments, de dispositifs médicaux et d'autres produits et objets réglementés dans l'intérêt de la santé publique.

Types d'industriels de santé :

- les entreprises pharmaceutiques ;
- les entreprises fabricant des dispositifs médicaux et des dispositifs médicaux de diagnostic *in vitro* ;
- les grossistes répartiteurs et dépositaires en médicaments ;
- les entités liées à la fabrication de produits sanguins.

2.3.4 Les fournisseurs et prestataires pour le secteur de la santé

Certains acteurs fournissent des services et/ou des biens aux entités du secteur de la santé tels que des services informatiques, des services « métier » ou encore certains équipements utilisés en milieu médical.

Types de fournisseurs et prestataires pour le secteur de la santé :

- les prestataires informatiques tels que les entreprises de services numériques (ESN), les infogérants, les hébergeurs, les fournisseurs de logiciels ou de solutions numériques ;
- les prestataires de services de paiement tels que les gestionnaires de tiers payant ;
- les fournisseurs d'équipements utilisés en milieu médical, par exemple à des fins logistiques.

3 QUELQUES CARACTÉRISTIQUES MAJEURES DU SECTEUR DE LA SANTÉ

Le secteur de la santé est un secteur hautement critique, soumis au triple impératif de disponibilité, de confidentialité et d'intégrité concernant les systèmes d'information (SI) utilisés et les données traitées. Les incidents d'origine informatique qui l'affectent peuvent avoir des conséquences importantes sur la continuité des soins et des services de santé, pouvant aller jusqu'à la mise en danger de la vie humaine. Un rapport de l'éditeur de sécurité PROOFPOINT et de l'INSTITUT PONEMON publié en 2023 [1] montrait ainsi que les attaques informatiques [2] affectant des entités du secteur de la santé, notamment les prestataires de soins, pouvaient entrainer des délais supplémentaires dans les procédures et tests médicaux et générer une augmentation de la durée des séjours à l'hôpital, des transferts d'établissements, des complications liées à des procédures médicales, et une hausse du taux de mortalité.

En France, le secteur est caractérisé par la fragmentation et l'hétérogénéité des acteurs qui le composent. Il se caractérise également par la numérisation progressive du processus de soins, à travers par exemple le Dossier Patient Informatisé (DPI) et le développement de services et de nouvelles technologies comme la télémédecine, les dispositifs médicaux connectés et la robotisation, qui augmentent sa surface d'exposition.

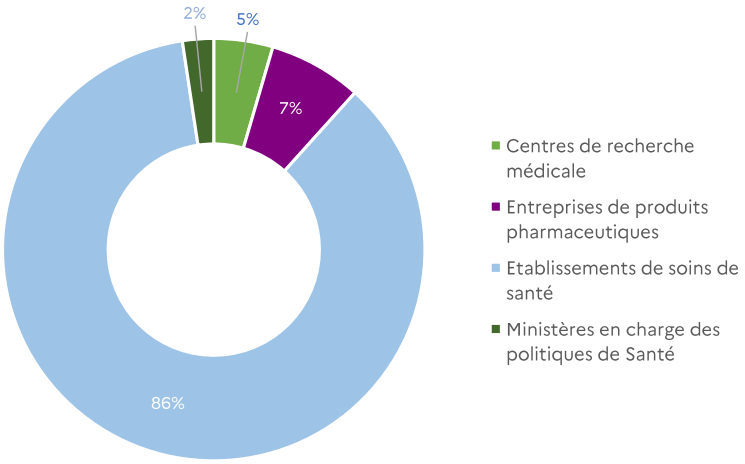

FIGURE 1 – *Distribution des incidents et signalements transmis à l'ANSSI entre janvier 2022 et décembre 2023 par entités du secteur de la santé*

2. Dans l'ensemble de ce document, les termes « attaque », « intrusion » ou « compromission » sont employés pour décrire une action offensive ayant mené à un effet concret sur la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données présentes sur un système d'information. Le terme « ciblage » est employé pour désigner une tentative d'intrusion informatique (par exemple, l'envoi d'un courriel de hameçonnage) ou des actions réalisées en amont d'une compromission.

Parmi les incidents[3] et signalements[4] transmis à l'ANSSI entre janvier 2022 et décembre 2023 dans le secteur de la santé, 86% concernaient des établissements de santé, 7% des organisations productrices de produits pharmaceutiques, 5% des centres de recherche médicale et 2% les ministères en charge des politiques de santé et leurs établissements publics. La part de ces événements dans le total des incidents ou signalements traités par l'Agence n'a cessé d'augmenter, passant de 2,87% en 2020, à 11,4% en 2023.

Un tiers des incidents touchant des établissements de santé observés par l'ANSSI en 2022 et 2023 concerne des compromissions de comptes de messagerie, parfois couplées à des envois de courriels d'hameçonnage. Ces événements sont de faible gravité lorsqu'ils restent circonscrits à quelques comptes à faible privilège et ne débouchent pas sur des actions supplémentaires, comme une élévation de privilège[5] ou une latéralisation[6]. Un autre tiers recouvre des activités à plus forts impacts telles que des chiffrements par rançongiciels et des exfiltrations de données ou encore des indisponibilités temporaires liées à des dénis de service. Le reste des incidents rassemble des comportements à risque d'utilisateurs (téléchargement de logiciels infectés, connexion de clé USB non maîtrisée, etc.) et des problèmes matériels tels que des pannes, ainsi que des compromissions par des codes malveillants aux conséquences très limitées.

Créé en 2017, le CERT-Santé[7] est à la fois en capacité d'assurer un suivi sectoriel des incidents et, dans le cas de crises à fort impact telles que des attaques par rançongiciel, de fournir un accompagnement dans la durée. Depuis 2021, la quasi-totalité des incidents de type rançongiciel est signalée au CERT-FR directement ou par l'intermédiaire du CERT-Santé dès leur détection, permettant ainsi une assistance rapide aux bénéficiaires.

3.1 Les établissements de santé

3.1.1 Particularités de l'informatique hospitalière

Au sein des établissements de santé, la prise en charge et le traitement de patients reposent sur des SI composés de nombreux services et applications interconnectés, notamment nécessaires pour la gestion des données des patients. Le plus souvent, ces services et applications ne sont pas résilients, en raison d'incompatibilité des logiciels utilisés, ou encore par manque de moyens. Leur interruption peut fortement perturber les capacités de prise en charge de patients et les services de soins. Lors des incidents traités par l'ANSSI, les services de réanimation, de pharmacie, de laboratoire et d'imagerie ont été particulièrement affectés par l'indisponibilité de l'infrastructure informatique. L'accès aux DPI est également très souvent affecté dès la mise

3. Un incident de sécurité est, dans la taxonomie de l'ANSSI, un évènement de sécurité pour lequel l'ANSSI confirme qu'un acteur malveillant a conduit des actions avec succès sur le système d'information de la victime.

4. Un signalement d'incident désigne toute description détaillée des caractéristiques techniques d'un ou plusieurs événements de sécurité susceptibles de conduire à la découverte d'un incident de sécurité survenu sur le système d'information d'une organisation donnée.

5. Une élévation de privilèges désigne l'obtention de privilège supérieur par exploitation d'une vulnérabilité. Par exemple, si un utilisateur local accède à des droits normalement réservés à l'administrateur, il y a élévation de privilège. Une élévation de privilège est souvent recherchée par une personne malveillante lorsqu'elle a réussi à s'introduire sur un système d'information en usurpant l'identité d'un utilisateur légitime.

6. La latéralisation désigne une phase durant laquelle un attaquant se déplace sur un réseau afin de chercher à compromettre d'autres ressources ou systèmes.

7. Hébergé au sein de l'Agence du Numérique en Santé (ANS), le CERT-Santé apporte depuis 2017 un accompagnement de cybersécurité en alerte et en réponse aux incidents à des entités prestataires de soins ou de services médico-sociaux, et travaille en relation avec le CERT national (CERT-FR) animé par l'ANSSI. Pour rappel, le Centre de réponse aux incidents cyber (*Computer Emergency Response Team* ou CERT) est un nom déposé et désigne une équipe de réponse aux attaques cyber.

en place des premières mesures d'endiguement à la découverte de l'incident. Par ailleurs, le SI est composé d'équipements spécialisés qui doivent avoir un accès à Internet et la dépendance croissante à des services cloud tels que des plateformes de prise de rendez-vous ou d'analyse d'imagerie médicale, nécessite des réouvertures de flux rapides dans le cadre de réponses à incident.

L'impératif de garantir la disponibilité des services pour de nombreux utilisateurs et applications se traduit fréquemment par des SI dépourvus de segmentation réseau et de contrôle d'accès. Ce manque de cloisonnement favorise la propagation de codes malveillants et le chiffrement généralisé des infrastructures numériques. Ces attaques informatiques peuvent affecter des SI liés à des services « métiers » mais également des SI de gestion bâtimentaire et ainsi nuire à la surveillance et à la sécurité physique des établissements de santé.

Comme pour des victimes d'autres secteurs, l'interdépendance des SI hospitaliers peut constituer un obstacle à la reprise progressive des services suite à une attaque informatique. En effet, la remise en route d'un service implique que l'infrastructure informatique sur laquelle il repose soit saine et nécessite d'effectuer des analyses sur l'intégralité des ressources dont il dépend. Pour les établissements de santé, l'allongement de la durée de ces vérifications a une incidence particulièrement notable, du fait de leur besoin important de continuité des services de soins.

En outre, l'utilisation de machines médicales spécialisées telles que des automates ou des objets connectés souvent peu sécurisés est également fréquente (voir la partie 3.2). Ces machines peuvent constituer des cibles facilement exploitables par des attaquants.

Les établissements de santé disposent également de nombreuses interconnexions et dépendances métier avec d'autres entités pouvant permettre à un attaquant de se latéraliser ou de provoquer des dommages collatéraux sur un périmètre plus large. Dans le cadre de réponses à incidents, l'ANSSI a ainsi fréquemment observé des attaques informatiques contre des centres hospitaliers ayant des effets indirects sur d'autres entités du fait de leur appartenance au même Groupement Hospitalier de Territoire (GHT), au même Groupement de Coopération Sanitaire (GCS) (EHPAD, crèches, etc.), ou encore sur des organismes nationaux tels que l'ÉTABLISSEMENT FRANÇAIS DU SANG (EFS). De surcroît, certains services étant mutualisés, leur indisponibilité peut perturber le fonctionnement d'autres établissements. Lors d'un incident récent, la perturbation d'un service de laboratoire a affecté d'autres entités d'un Groupement de Coopération Sanitaire (GCS), celui-ci menant des analyses à leur profit. Le fonctionnement des établissements de santé repose par ailleurs sur de nombreux fournisseurs et prestataires dont la compromission peut perturber le fonctionnement de l'établissement ou permettre des attaques *via* la chaine d'approvisionnement.

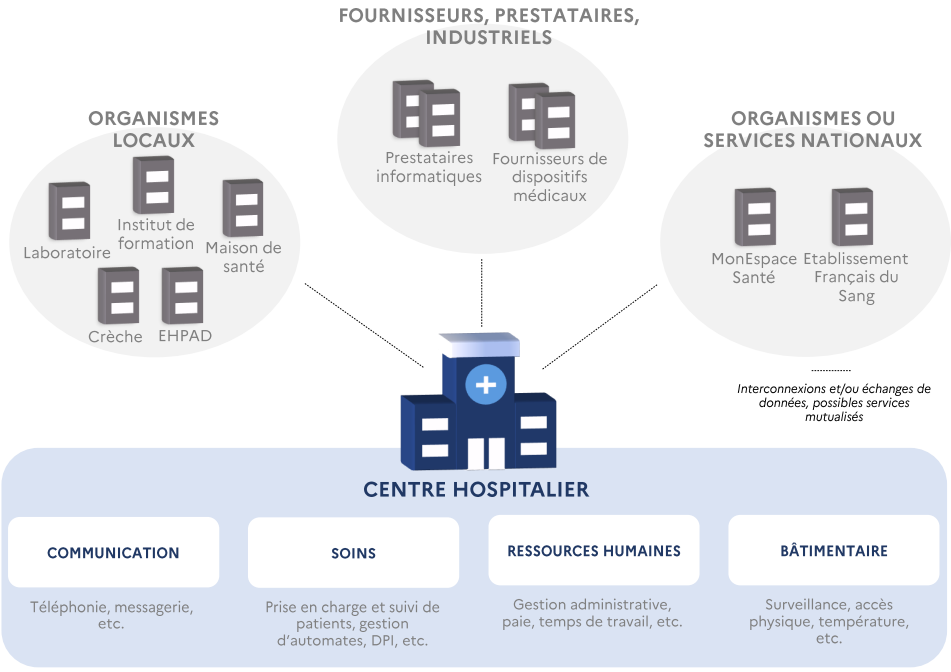

FIGURE 2 – *Quelques fonctions et dépendances critiques d'un Centre Hospitalier typique*

3.1.2 Contraintes structurelles des établissements de santé

Outre ces particularités informatiques, l'ANSSI relève également des contraintes structurelles notables pour les établissements de santé en France :

- des budgets et effectifs contraints entrainant une moindre maitrise du SI et de son architecture ainsi que des difficultés de maintien en condition de sécurité ;
- des difficultés dans la mise en oeuvre des opérations de maintenance informatique, en raison de la forte contrainte structurelle de disponibilité des SI ;
- la complexité de maintenance de certains dispositifs médicaux, notamment « lourds » tels que les scanners, dont le parc n'est pas souvent renouvelé et dont le maintien en condition de sécurité n'est pas réalisable par l'établissement de santé (voir le paragraphe 3.2) ;
- un déséquilibre de la relation entre petites structures et fournisseurs de services ou d'équipements informatiques, qui peut engendrer des mauvaises pratiques de sécurité. À titre d'exemple, des délégations de droits trop larges pour l'administration de SI peuvent être demandées par certains prestataires ;
- même si des progrès significatifs ont été constatés, la persistance de mauvaises pratiques d'hygiène informatique telles que le recours à du matériel personnel pour administrer des SI, notamment en raison d'un manque de moyens dédiés aux équipes informatiques.

Commentaire : pour répondre à certaines difficultés, notamment budgétaires, un mouvement de mise en commun des ressources humaines et des systèmes informatiques des établissements de santé peut être observé à travers les GHT. Toutefois, cette mutualisation introduit des risques supplémentaires comme l'indisponibilité de l'ensemble des SI mis en commun en cas d'incident informatique. La sensibilité des SI mutualisés au sein des GHT implique ainsi de les administrer de façon sécurisée, en s'appuyant sur des ressources humaines et financières adaptées.

Pour répondre plus largement aux besoins de sécurisation rencontrés par les établissements

de santé, l'ANSSI rappelle également que des actions destinées à rehausser le niveau de cybersécurité des établissements de santé français ont été mises en œuvre depuis 2020. Ainsi, de nombreuses entités ont pu bénéficier d'accompagnements de proximité dans le cadre du programme « parcours de cybersécurité » développé dans le contexte de France Relance (2020-2022) et piloté par l'ANSSI, ou encore du programme Cybersécurité accélération et Résilience des Etablissements ou CaRE (2023-2027) [2, 3]. L'ANSSI met à disposition de nombreux bénéficiaires les services d'audits automatisés ADS pour les annuaires *Active Directory*[8], et SILENE pour l'exposition sur Internet. En 2024, des ajustements ont également été apportés au référentiel de certification des établissements de santé de la Haute Autorité de Santé, afin de renforcer les exigences sur la thématique du numérique en santé, notamment les critères liés à la gestion du risque numérique et à la promotion de bons usages relatifs à l'utilisation des outils numériques comme MonEspaceSanté et aux données des patients [4]. La directive NIS 2 devrait par ailleurs constituer un levier pour les Responsables de la Sécurité des Systèmes d'Information (RSSI) d'établissements de santé, en leur permettant de faciliter la visibilité des sujets de cybersécurité auprès de leur direction et de bénéficier d'une cible de sécurité commune dans le cadre de la mutualisation des SI au niveau des GHT.

3.2 Les dispositifs médicaux connectés et autres équipements sensibles utilisés en milieu médical

L'ANSSI identifie également des risques de sécurité liés aux dispositifs médicaux[9] connectés. En effet, ces derniers ne sont globalement pas tenus à jour, car ils sont le plus souvent certifiés pour ne fonctionner que sur une version d'un système d'exploitation et achetés sans contrat incluant leur maintien en condition de sécurité sur toute la durée de vie de l'équipement. La dépendance à des dispositifs obsolètes peut ainsi nuire au niveau de sécurité global des SI. Par exemple, un dispositif médical ne pouvant être administré que par un système d'exploitation obsolète peut contribuer plus largement à l'obsolescence d'une partie du parc informatique qui ne peut plus être mis à jour pour ne pas compromettre le bon fonctionnement du dispositif médical.

Les dispositifs médicaux connectés peuvent également être affectés par des vulnérabilités jour zéro[10], qui pourraient être exploitées par des attaquants comme vecteur d'accès initial pour obtenir des accès non autorisés à des données ou à d'autres SI interconnectés, ou encore pour altérer le fonctionnement du dispositif médical lui-même. À titre d'exemple, en septembre 2022, le fabricant de technologies médicales MEDTRONIC a rapporté une vulnérabilité affectant ses modèles de pompes à insuline MiniMed 600. Cette vulnérabilité, liée au protocole de communication entre la pompe à insuline et différents composants sans fil (émetteur de surveillance continue du glucose (CGM), lecteur de glycémie et *USB CareLink*), pouvait permettre à un attaquant d'obtenir un accès non autorisé à une pompe à insuline MiniMed 600 et d'augmenter ou de baisser le dosage d'insuline administré [5]. Le même mois, le Federal Bureau of Investigation (FBI) a également émis une alerte concernant les risques d'attaques informatiques contre

8. L'*Active Directory* est un service d'annuaire de l'éditeur MICROSOFT permettant la gestion centralisée de comptes, de ressources et de permissions.

9. Aux termes de l'article 2 du règlement européen 2017/145, le terme dispositif médical désigne un produit destiné à être utilisé seul ou en association chez l'homme à des fins de diagnostic, de prévention, de contrôle, de prédiction, de pronostic, de traitement, d'atténuation d'une maladie, d'une blessure ou d'un handicap, de communication d'informations, d'investigation, de remplacement ou de modification d'une structure ou d'une fonction anatomique, d'un processus ou d'un état physiologique ou pathologique.

10. Une vulnérabilité jour zéro est une vulnérabilité n'ayant fait l'objet d'aucune publication ou n'ayant reçu aucun correctif.

les appareils médicaux obsolètes, en évoquant entre autres des dispositifs médicaux tels que les pompes à insuline, les défibrillateurs intracardiaques, la télémétrie cardiaque mobile, les stimulateurs cardiaques ou encore les pompes à douleur intrathécales [6].

L'ANSSI relève plus largement des risques de sécurité liés à certains équipements utilisés en milieu médical, par exemple à des fins logistiques, qui peuvent également être affectés par des vulnérabilités dont l'exploitation à des fins malveillantes a le potentiel de générer des conséquences sur le bon fonctionnement d'activités médicales. Ainsi, en mai 2021, l'entreprise de sécurité informatique ARMIS, a alerté l'entreprise SWISSLOG, spécialisée dans les solutions d'automatisation de la chaîne logistique, de l'existence de multiples vulnérabilités critiques dans son système de transport pneumatique (*Swisslog PTS*), destiné aux hôpitaux. Ce système permettrait notamment d'automatiser la logistique et le transport de ressources telles que les médicaments ou encore les produits sanguins, à travers un réseau de tubes pneumatiques au sein des hôpitaux. Ces vulnérabilités auraient pu permettre à un attaquant de prendre le contrôle du réseau de tubes pneumatiques d'un hôpital sans authentification. Parmi les risques notables identifiés par l'entreprise de sécurité ARMIS, un attaquant aurait pu manipuler les commandes permettant de gérer la vitesse de transport au sein des tubes pneumatiques, et ainsi compromettre certains produits sensibles, tels que les produits sanguins, qui doivent être transportés avec précaution pour ne pas être endommagés [7, 8].

4 MENACE À FINALITÉ LUCRATIVE

La menace cybercriminelle à des fins lucratives constitue la principale menace pesant sur les entités du secteur de la santé. Elle peut prendre plusieurs formes : attaques par rançongiciel, exfiltration de données à des fins de revente, ou emploi de diverses techniques de fraude comme l'usage de faux sites web, l'usurpation de marque et la compromission de systèmes informatiques pour escroquer ou détourner des sommes d'argent.

4.1 Attaques par rançongiciel à des fins d'extorsion

Depuis 2020, le secteur de la santé a continué à être la cible d'attaques par rançongiciel. Au cours de la pandémie de Covid-19, de nombreux opérateurs de rançongiciel ont tiré profit de la pression pesant sur le secteur de la santé, contraint par un besoin encore plus important que d'ordinaire de continuité opérationnelle et d'adaptation [9].

Toutefois, de manière générale, le secteur de la santé n'apparait pas être une cible spécifique des opérateurs de rançongiciels, qui semblent majoritairement agir de manière opportuniste contre des entités vulnérables de toute nature.

Commentaire : la visibilité des incidents touchant les entités du secteur de la santé, notamment les établissements de santé, pourrait être en partie liée aux exigences légales de signalement auxquelles elles sont soumises. Elle pourrait également être liée à la couverture médiatique plus importante reçue par les structures accueillant du public lorsqu'elles sont victimes d'incidents. Cette visibilité tend à favoriser une perception de ciblage important du secteur de la santé. Il en demeure cependant que le niveau de sécurité variable des entités du secteur et notamment des SI hospitaliers, favorise leur ciblage.

Les attaques par rançongiciel peuvent entrainer l'indisponibilité de certains services et/ou données et ralentir, voire arrêter l'activité de l'entité compromise. Elles s'accompagnent souvent d'exfiltrations de données que les cybercriminels menacent de divulguer en cas de non-paiement de la rançon : il s'agit du principe de la double extorsion. Dans certains cas, les opérateurs de rançongiciel peuvent également exfiltrer des données et exercer un chantage à la divulgation sans nécessairement procéder au chiffrement des systèmes informatiques.

Ces attaques peuvent également avoir des conséquences à la fois en matière de réputation mais aussi légales et financières pour les entités touchées. Lorsqu'elles ciblent des acteurs liés à la fourniture de soins de santé, les attaques par rançongiciel peuvent également avoir des conséquences sur la sécurité des patients. Une étude publiée en octobre 2023 par des chercheurs de l'UNIVERSITÉ DU MINNESOTA portant sur les conséquences des attaques par rançongiciel sur les hôpitaux a ainsi montré que ce type d'intrusion informatique pouvait augmenter le risque de mortalité des patients déjà admis au moment de l'attaque [10].

Si ces attaques sont majoritairement conduites par des acteurs cybercriminels, elles peuvent également être menées par des acteurs étatiques à des fins lucratives. À titre d'exemple, en juillet 2024, le DEPARTMENT OF JUSTICE des États-Unis a mis en accusation un opérateur associé au MOA réputé nord-coréen Andariel, pour son rôle dans la compromission d'entités du secteur de la santé dans le but de déployer des rançongiciels, blanchir les rançons obtenues, et financer ainsi des opérations offensives ultérieures contre des entités gouvernementales, de la défense et des technologies à travers le monde [11, 12, 13].

4.1.1 Attaques par rançongiciel contre des prestataires de soins

4.1.1.1 Établissements de santé

Depuis 2020, de nombreux établissements de santé français ont été victimes d'attaques par rançongiciel ayant entrainé des des exfiltrations de données et des perturbations importantes liées à la continuité des soins et à la prise en charge des patients. En 2022 et 2023, l'ANSSI a été informée de 30 compromissions et chiffrements par des rançongiciels ayant affecté des établissements de santé. Ces incidents représentent 10% des incidents liés à des rançongiciels signalés à l'ANSSI sur cette période.

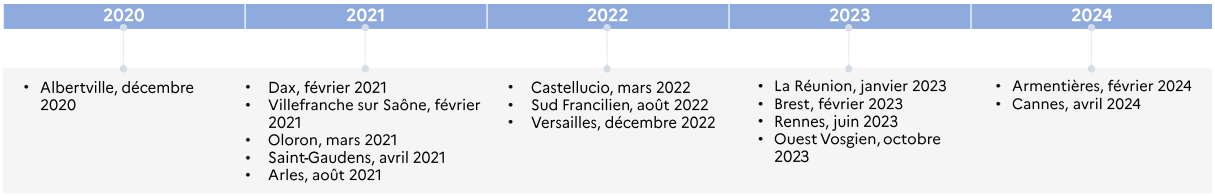

FIGURE 3 – *Exemples d'attaques par rançongiciel ayant touché des centres hospitaliers en France depuis 2020*

Lors des investigations menées suite à ces incidents, les souches de rançongiciel suivantes ont été observées : Lockbit (dont Lockbit 3.0), NoEscape, Bitlocker, Bianlian, Phobos, Blackcat, Blackhunt, Wannacry, Scarab et ViceSociety. Les établissements de santé ne semblent ainsi pas ciblés par les opérateurs d'un rançongiciel en particulier. Certains groupes cybercriminels semblent parfois mettre en œuvre des outils spécifiques à leurs cibles, avec notamment l'utilisation de dictionnaire de mots de passe ayant trait au domaine médical.

Une fois le SI compromis, les attaquants réussissent majoritairement à chiffrer tout ou partie des systèmes. Dans certains cas, les outils de détection identifient des comportements malveillants à temps et empêchent le chiffrement du parc informatique [14]. Par ailleurs, les attaquants ne procèdent pas systématiquement à des exfiltrations de données et les menaces de publication de données ne sont pas toujours suivies d'effet.

Concernant le vecteur d'intrusion initiale, dans la majorité des cas observés et quand celui-ci a pu être identifié, les attaquants parviennent à pénétrer les réseaux des établissements *via* la compromission de comptes Virtual Private Network (VPN) ou réseau privé virtuel[11] appartenant à des prestataires ou à des personnels dont les comptes ne sont plus utilisés.

Selon les observations de l'ANSSI, les sauvegardes sont souvent ciblées et parfois effacées par les attaquants pour perturber les capacités de reconstruction des victimes et accentuer la pression pour le paiement de rançons. Dans au moins un cas, un attaquant a tenté de rendre inopérant un mécanisme de verrouillage temporaire ou *time-lock* afin de complexifier l'exploitation des sauvegardes d'un établissement en stoppant la réplication et en chiffrant les copies existantes. Les serveurs de gestion des machines virtuelles font également l'objet d'un intérêt particulier pour les attaquants qui y voient une opportunité rapide de chiffrer rapidement des ressources métiers essentielles.

11. Ces comptes VPN peuvent être compromis *via* l'utilisation d'authentifiants légitimes compromis ou encore suite à l'exploitation de vulnérabilités.

Le cas du CENTRE HOSPITALIER SUD-FRANCILIEN

Dans la nuit du 20 au 21 août 2022, le CENTRE HOSPITALIER SUD FRANCILIEN, qui assure la couverture sanitaire d'environ 700 000 habitants [15], a été compromis au moyen du rançongiciel Lockbit 3.0, opéré par le groupe cybercriminel Lockbit selon le modèle économique du *ransomware-as-a-service* (RaaS)[a]. Les attaquants ont exigé une rançon de dix millions de dollars en échange du déchiffrement des systèmes informatiques touchés [16].
Cette compromission a entrainé des impacts métiers significatifs : les personnels hospitaliers ont notamment fait état de perturbations sur des services de messagerie, de pharmacie, ou encore de comptabilité et de ressources humaines. Dans ce contexte, des nouveaux-nés du service de néonatalogie ont dû être transférés vers d'autres établissements et l'indisponibilité de certains automates de laboratoires a perturbé la capacité à réaliser des analyses biologiques [17]. Par ailleurs, l'entité a également été victime d'une exfiltration de onze gigaoctets de données qui ont été publiquement divulgués le 23 septembre 2022. Ces données incluaient notamment des données de santé et personnelles de patients, de membres du personnel et de partenaires de l'hôpital [15].

a. Un *ransomware-as-a-service* ou rançongiciel en tant que service est livré prêt à l'emploi par une organisation cybercriminelle et mis à disposition d'affiliés, même novices en programmation, contre le partage de la rémunération.

L'ANSSI a également eu connaissance depuis 2020 d'attaques par rançongiciel aux impacts significatifs contre des établissements de santé à l'étranger.

À titre d'exemple, en décembre 2023, dans le cadre d'une attaque par rançongiciel contre le centre de traitement des cancers FRED HUTCHINSON à Seattle aux États-Unis, le groupe cybercriminel et opérateur de RaaS Hunters International a exigé le paiement d'une rançon à l'entité visée en échange de la non-publication des données dérobées mais également à certains patients individuellement, en réclamant cinquante dollars contre la suppression de leurs informations [18].

Plus récemment, une attaque au moyen du rançongiciel BlackBasta, opéré par un groupe cybercriminel selon le modèle du RaaS, a affecté le réseau hospitalier américain ASCENSION HEALTH en mai 2024 suite au téléchargement par un employé d'une pièce jointe malveillante issue d'un courriel de hameçonnage. L'intrusion informatique a causé l'indisponibilité de certains systèmes téléphoniques et de commande de tests, de procédures et de médicaments et a également affecté l'application *MyChart*, utilisée par les patients pour consulter leurs dossiers de santé électroniques et communiquer avec des fournisseurs de soins [19]. Ces indisponibilités ont entrainé un retour à des prises en charge entièrement manuelles et non informatisées pour le suivi des procédures et de l'administration de médicaments, la mobilisation des patients pour qu'ils mettent à l'écrit leurs informations médicales, la suspension des procédures, des tests et des rendez-vous non urgents et la redirection des cas urgents vers les services médicaux d'urgence. Un mois après l'incident, des perturbations étaient encore rapportées, telles que des erreurs de médication, des retards et des pertes de résultats médicaux [20, 21, 22].

4.1.1.1.1 Remédiation des attaques par rançongiciel contre les établissements de santé

La remédiation des attaques par rançongiciel et le retour au mode de fonctionnement nominal peut durer jusqu'à plusieurs mois et générer des coûts élevés liés à la réponse à incident, à la reconstruction des SI touchés, aux pertes de recettes ou encore aux ressources humaines

mobilisées. À titre d'exemple, le coût total estimé de l'attaque par rançongiciel ayant touché le CENTRE HOSPITALIER SUD FRANCILIEN en août 2022 se serait élevé à 7 millions d'euros [23].

Au vu de la complexité et de la porosité des SI hospitaliers, les actions de remédiation sont menées sur le long cours. De fait, certains services subissent toujours les conséquences de la crise un an après le début de l'incident. La disponibilité de sauvegardes intègres conditionne la reprise d'activité et varie en fonction du type de stockage choisi. La reconstruction du SI nécessitant fréquemment de nouvelles machines [12], le manque de stock ou les délais de commande peuvent fortement affecter le calendrier de la reprise d'activité.

Outre l'intervention de prestataires spécialisés en réponse à incident et l'achat de matériels neufs pour la reprise d'activité, la relance des machines spécifiques, dont la configuration est souvent connue par un nombre réduit d'acteurs, peut nécessiter le concours de prestataires spécialisés pouvant ralentir de manière importante la reconstruction du reste du système d'information et engendrer des coûts supplémentaires.

Enfin, il a été observé que les budgets alloués à la sécurité informatique progressent mais restent insuffisants. En outre, les établissements de santé peinent à recruter ou former des personnels compétents dans le domaine de la sécurité des SI, ce qui rend complexe la poursuite des opérations de remédiation entreprises pendant la crise et les mesures nécessaires au renforcement du niveau de sécurité. Dans certains cas, les établissements parviennent toutefois à disposer des ressources suffisantes pour durcir leur SI et mettre en place des dispositifs de supervision.

Commentaire : certains établissements de santé remédient particulièrement efficacement les attaques par rançongiciel, mais la majorité rencontre de fortes difficultés. In fine, l'efficacité de la remédiation repose souvent sur le personnel disponible au sein de ces entités et sur la bonne connaissance des SI concernés. La gestion d'un incident grave se conclut généralement par une amélioration de la cybersécurité de l'établissement (segmentation réseau, mise en place de dispositif de supervision, etc.) et une meilleure implication de l'ensemble des personnels et de la direction.

Gestion de crise au sein des établissements de santé

En matière de gestion de crise, les établissements de santé disposent d'un « plan blanc » définissant les modalités de gestion de crise ainsi que les moyens permettant de continuer ses activités de manière dégradée. Rendu obligatoire dès 2004, il a été fortement éprouvé pendant la crise sanitaire liée à la Covid-19 et est mis en pratique rapidement dès qu'un événement de grande ampleur, affectant le fonctionnement de l'établissement, est détecté. Ce plan organise notamment la constitution de cellules de crise, les modalités de passage en fonctionnement dégradé des activités (délestages de patients vers d'autres établissements, reports des consultations et opérations non urgentes, etc.). Depuis 2023, ce plan intègre un volet spécifique aux incidents cyber qui prévoit les éléments à préparer en amont de la crise cyber et les mesures organisationnelles spécifiques à appliquer lorsqu'elle survient. Son application, même partielle, permet aux organisations de gagner un temps précieux dans les premiers instants de la crise.

4.1.1.2 Laboratoires d'analyse médicale

L'ANSSI a observé des ciblages de laboratoires d'analyse médicale par des attaques par rançongiciel conduisant à l'indisponibilité de certaines capacités critiques pour la délivrance de soins, telles que les capacités de test et de diagnostic médical. De telles attaques ont des effets directs

12. Une partie des machines compromises ne peut pas être réutilisée dans un premier temps car mise sous séquestre pour l'enquête judiciaire ou en cours d'investigations.

sur l'activité des prestataires de soins, qui ont besoin de s'appuyer sur ces capacités pour effectuer des opérations ou encore prescrire des traitements. En outre, les attaques par rançongiciel contre des laboratoires d'analyse médicale peuvent également entrainer des fuites de données sensibles telles que des données médicales ou personnelles de patients.

Ainsi, en juin 2024, le fournisseur britannique de services de pathologie SYNNOVIS a été victime d'une attaque au moyen du rançongiciel du groupe cybercriminel Qilin, opéré suivant le modèle du RaaS. L'attaque informatique a causé l'indisponibilité d'un service de test nécessaire pour les transfusions sanguines. Cette indisponibilité a eu d'importantes conséquences opérationnelles sur de nombreux hôpitaux au Royaume-Uni, en entrainant par exemple des annulations de rendez-vous patients et d'opérations chirurgicales vitales, des transferts vers d'autres établissements, et en générant une pression sur les stocks de sang des groupes O positif et O négatif. La compromission informatique a également occasionné une fuite de près de quatre cents gigaoctets de données incluant notamment des données personnelles de patients [24, 25, 26].

4.1.2 Attaques par rançongiciel contre des prestataires de services pour le secteur de la santé

4.1.2.1 Prestataires informatiques

Les prestataires informatiques peuvent proposer des prestations et des solutions destinées à une clientèle sectorielle large ou spécifiquement destinées à des clients du secteur de la santé. Ainsi, leur compromission a le potentiel d'entrainer des perturbations opérationnelles et des fuites de données pouvant affecter en cascade de multiples clients.

En janvier 2024, l'ANSSI a été informée de la compromission d'un prestataire numérique français proposant notamment des services de télémédecine à des prestataires de soins. Le prestataire a été compromis au moyen du rançongiciel Lockbit 3.0 qui a causé l'indisponibilité de sa plateforme *software-as-a-service* (SaaS). Cette compromission était liée à l'exploitation d'une vulnérabilité sur un serveur CITRIX, qui a permis à l'attaquant de récupérer les informations d'authentification d'un compte. L'indisponibilité de cette plateforme a perturbé le fonctionnement des établissements de santé clients de ce prestataire et notamment entrainé le transfert de patients en urgence vers d'autres établissements.

4.1.2.2 Prestataires de services de paiement

Les prestataires de services de paiement sont chargés de la gestion externalisée de transactions de santé. Leur indisponibilité peut ainsi perturber les capacités de vérification et de paiement des acteurs du secteur et entrainer l'exposition de données sensibles telles que des données personnelles ou encore bancaires de patients ou de professionnels de santé.

En février 2024, l'attaque par rançongiciel ayant touché le gestionnaire de transactions de santé américain CHANGE HEALTHCARE, en charge de la gestion de plusieurs milliards de transactions de soins par an, en est une illustration pertinente. CHANGE HEALTHCARE a ainsi été la victime du rançongiciel Blackcat, opéré par un groupe cybercriminel suivant le modèle du RaaS. Cette attaque a affecté les capacités de facturation, de transmission des réclamations d'assurance, de vérification des couvertures santé, et de traitement des ordonnances de nombreux prestataires de soins aux États-Unis. L'attaque a également entrainé l'exfiltration de six téraoctets de données, dont des données personnelles, médicales et de paiement. Les pertes financières estimées relatives à l'incident s'élevaient à huit cent soixante-douze millions de dollars pour le premier trimestre 2024. L'attaquant aurait utilisé des authentifiants dérobés pour se connecter

sur un portail d'accès à distance CITRIX pour lequel l'authentification multifactorielle n'était pas activée. Suite à cet incident, CHANGE HEALTHCARE aurait payé la rançon exigée par les cybercriminels. Toutefois, quelques mois plus tard, l'entité a à nouveau été victime d'un chantage à la divulgation émanant d'un autre groupe cybercriminel qui prétendait être également en possession de données exfiltrées en février 2022 suite à un conflit interne entre cybercriminels [27, 28, 29].

Commentaire : cette seconde tentative d'extorsion, à quelques mois d'intervalle, met une nouvelle fois en évidence que le paiement d'une rançon dans le contexte d'une attaque par rançongiciel ne permet pas nécessairement à une entité de se prémunir contre de nouvelles attaques.

4.1.3 Attaques par rançongiciel contre des industriels de produits de santé

Des attaques par rançongiciel ont également affecté des industriels du secteur de la santé depuis 2020, entrainant notamment, parmi les conséquences les plus notables, des ralentissements, voire des arrêts de la production de certains produits de santé ou encore des fuites de données liées à des secrets industriels.

En juin 2024, LES LABORATOIRES ETHYPHARM, filiale française du groupe pharmaceutique européen ETHYPHARM, spécialisé dans les pathologies du Système Nerveux Central (SNC) et les injectables hospitaliers, aurait été victime d'une fuite de données suite à une attaque par rançongiciel revendiquée par le groupe cybercriminel Underground Team [13]. Le groupe cybercriminel avait notamment revendiqué avoir exfiltré des données liées aux ressources humaines et des informations confidentielles dont des secrets industriels [31].

En juillet 2024, le fournisseur de sang américain ONEBLOOD, fournisseur de nombreux établissements de santé localisés dans le sud-est des États-Unis, a été la cible d'une attaque par rançongiciel. Cette attaque a entrainé un ralentissement opérationnel notamment lié à un retour à des procédures manuelles pour étiqueter les produits sanguins, et une pression sur les stocks de sang de ONEBLOOD. L'attaque a également eu des conséquences indirectes dans plus de deux cent cinquante hôpitaux qui ont dû activer leurs protocoles d'urgence de pénurie de sang.

Commentaire : les incidents ayant touché ONEBLOOD ou encore SYNNOVIS mettent en exergue le rôle critique des produits sanguins pour la dispense de soins au sein des établissements de santé et les effets significatifs, pouvant aller jusqu'à la pénurie, que peuvent entrainer une attaque par rançongiciel contre des fournisseurs de produits sanguins ou des laboratoires chargés d'effectuer des tests sanguins.

4.2 Exfiltration de données à des fins de revente

Les entités du secteur de la santé sont détentrices de données de nature variée, qui incluent des données personnelles, médicales, d'authentification, de paiement, et stratégiques (données comptables, données liées au savoir-faire de l'entité, etc.). Ces données, du fait de leur sensibilité, ont une valeur importante à la revente.

Elles peuvent être dérobées à des fins de revente à d'autres acteurs cybercriminels sur des forums, *marketplaces* ou « places de marché criminelles », boutiques en ligne sur le *darknet* ou encore sur des plateformes de messagerie [32]. Les données sensibles ainsi revendues peuvent être

13. Le groupe cybercriminel Underground Team a été associé en source ouverte aux opérateurs du MOA Storm-0978 *aka* RomCom, qui auraient pratiqué des activités cybercriminelles et d'espionnage [30].

utilisées pour conduire d'autres attaques informatiques ou encore à des fins de fraude. À titre d'exemple, en mai 2024, un acteur cybercriminel nommé « Ansgar » aurait mis en vente sur un forum du *darknet* près de sept téraoctets de données personnelles et médicales de citoyens australiens exfiltrées des systèmes de MEDISECURE, prestataire australien de services de prescription électronique, pour la somme de cinquante mille dollars. Les données incluaient entre autres des noms et prénoms, adresses, numéros de téléphones et d'assurance, informations de prescription, courriels, authentifiants au site web de MEDISECURE. Ces données auraient potentiellement été dérobées lors d'une précédente intrusion informatique qui avait visé l'entreprise au début du mois de mai 2024 [33].

Certaines exfiltrations de données affectant le secteur de la santé ont une ampleur massive. L'année 2023 et le début de l'année 2024 ont été marqués par des incidents touchant notamment des acteurs du tiers payant. En effet, certains services en ligne traitant des données personnelles d'usagers ont été victimes d'exfiltrations massives de données [34]. Les attaquants exploitent la fragilité de l'authentification à ces plateformes (par exemple, l'absence de mesure de *rate-limiting* ou limitations de consultation), le grand nombre d'utilisateurs et le large accès octroyé aux utilisateurs à privilèges. Les authentifiants peuvent être récupérés *via* des campagnes d'hameçonnage ou sur des sites de revente d'authentifiants de connexion. Depuis ces comptes, des actions légitimes de consultation des bases de données permettent d'en exfiltrer le contenu. L'absence de supervision ou le manque de journalisation sont également des facteurs facilitant les compromissions. Les équipes techniques ne sont alors pas en mesure de détecter les comportements suspects ou bien le réalisent trop tardivement.

Ainsi, en février 2024, les opérateurs français spécialisés dans la gestion du tiers payant VIAMEDIS et ALMERYS ont été victimes d'attaques informatiques qui ont entrainé la fuite de données personnelles de plus de trente-trois millions de personnes, soit près de la moitié de la population française. Les données personnelles incluaient notamment l'état civil, la date de naissance, le numéro de sécurité sociale, le nom de l'assureur et les garanties du contrat des assurés [35].

Commentaire : la finalité précise liée aux fuites de données ayant affecté les prestataires de services Viamedis et Almerys en février 2024 demeure pour le moment inconnue. Toutefois, les données exfiltrées pourraient vraisemblablement être revendues ou exploitées à des fins de fraude.

En outre, le secteur de la santé n'est pas épargné par certains acteurs cybercriminels spécialisés dans la vente illégale de données d'authentification pour accéder au contrôle de machines à distance, à des interfaces d'administration (*control panels*), ou encore à des VPN. Ces acteurs sont également connus sous le nom de « courtiers en accès initiaux » [36, 37]. Ainsi, en décembre 2020, un acteur cybercriminel nommé « fooble » mettait en vente des données d'authentification à des comptes Citrix appartenant à un prestataire de soins canadien, avec une enchère de départ fixée à quatre mille dollars [32].

Au-delà des exfiltrations de données, le secteur de la santé peut également être exposé à des fuites accidentelles de bases de données qui peuvent être exploitées ultérieurement de manière malveillante. En février 2021, un manque de sécurisation de l'entreprise française DEDALUS BIOLOGIE a ainsi causé la fuite de données personnelles et de santé de près d'un demi-million de personnes. L'entreprise a été condamnée à payer 1,5 millions d'euros d'amende par la Commission Nationale pour l'Informatique et les Libertés [9].

4.3 Compromissions à des fins de fraude

Des faux documents ou produits de santé peuvent être vendus *via* des sites web frauduleux ou suite à la compromission d'entités du secteur de la santé. À titre d'exemple, entre août et sep-

tembre 2021, des cybercriminels ont compromis les comptes professionnels de quinze pharmaciens implantés dans la région Grand Est en France et édité puis revendu 6297 faux passes sanitaires pour des prix allant de cent à quatre-cent euros [38].

Des données de paiement ou des sommes d'argent peuvent également être dérobées à des clients et/ou patients d'entités du secteur de la santé victimes d'usurpations. En mars 2021, des domaines frauduleux qui usurpaient des sites web légitimes de l'entreprise pharmaceutique PFIZER et du FONDS DES NATIONS-UNIES POUR L'ENFANCE ont ainsi été saisis par la justice américaine. Certains domaines saisis cherchaient entre autres à tromper les visiteurs afin qu'ils soumettent des données personnelles et de paiement [39]. De la même manière, en septembre 2023, des individus soupçonnés d'avoir envoyé des SMS usurpant l'identité de l'ASSURANCE MALADIE et destinés à dérober les coordonnées bancaires de victimes ont été interpellés en France [40]. Le site web de l'ASSURANCE MALADIE met par ailleurs en garde contre le risque d'usurpation pouvant notamment s'appuyer sur l'envoi de faux SMS liés par exemple à la mise à jour de cartes vitales ou à des faux remboursements en attente et destinés à tromper les assurés pour leur dérober des informations de nature variée [41].

Par ailleurs, les entités du secteur de la santé peuvent également être victimes de virements frauduleux. En septembre 2022, le FEDERAL BUREAU OF INVESTIGATION a rapporté plusieurs cas de compromission de systèmes et services de paiement d'entités du secteur de la santé à des fins de détournement. À titre d'exemple, en février 2022, un cybercriminel aurait remplacé les coordonnées bancaires d'un hôpital par les coordonnées d'un compte bancaire lui appartenant, entrainant une perte de 3,1 millions de dollars pour la victime. Le FBI a notamment identifié l'exploitation par les cybercriminels d'authentifiants compromis et de techniques d'ingénierie sociale pour réaliser ce type d'attaques [42].

5 MENACE À FINALITÉ D'ESPIONNAGE

Les entités du secteur de la santé peuvent être la cible d'attaques informatiques à des fins d'espionnage conduites par des opérateurs de MOA réputés liés aux intérêts stratégiques d'États. Ces attaques informatiques sont menées dans le but d'obtenir des données personnelles et/ou médicales d'individus ou des données liées à la recherche médicale et au développement de technologies de santé. Ces données peuvent être dérobées à des fins de renseignement stratégique ou économique, afin de compenser des retards sur des sujets de santé spécifiques, de réduire les coûts de développement, d'obtenir des avantages concurrentiels ou encore de servir à des opérations ultérieures.

Si la crise sanitaire liée à la pandémie de Covid-19 a permis d'observer des activités d'espionnage informatique associées à des MOA réputés étatiques et menées contre le secteur de la santé, le secteur ne semble toutefois pas constituer une cible spécifique de ce type d'opérations. En effet, le ciblage du secteur de la santé s'inscrit souvent dans des campagnes d'espionnage plus larges, qui affectent des entités de secteurs variés.

Des évènements sanitaires majeurs, tels que la pandémie de Covid-19, peuvent ainsi constituer pour le secteur de la santé un contexte d'accentuation des activités d'espionnage informatique.

5.1 Ciblage d'entités du secteur de la santé dans le contexte de la crise sanitaire liée à la Covid-19

Les industriels de produits de santé, voire plus largement les acteurs liés à la recherche médicale, peuvent être spécifiquement ciblés par des opérations d'espionnage destinées à collecter des données de recherche ou sur le développement de technologies médicales. Ainsi, dans le contexte de la pandémie de Covid-19, marqué par un climat de concurrence vaccinale, plusieurs MOA réputés étatiques auraient été utilisés pour notamment cibler des données liées aux recherches sur la Covid-19, sur les vaccins et traitements développés ou encore sur les stratégies sanitaires nationales mises en œuvre.

Ainsi, entre mars et juin 2020, des individus travaillant au sein du secteur pharmaceutique aux États-Unis auraient été ciblés par des courriels de hameçonnage distribués par les opérateurs du MOA réputé iranien APT42, à des fins de collecte d'authentifiants. Les attaquants auraient notamment usurpé des services légitimes de GOOGLE et YAHOO, ou encore l'identité d'un chercheur en vaccins de l'université d'Oxford. Ces ciblages du secteur de la santé auraient reflété un changement temporaire de la victimologie associée au MOA APT42, potentiellement en lien avec la pandémie [43]. Ce type de ciblage n'a pas été observé au-delà de l'année 2020. En outre, l'agence de presse REUTERS a rapporté en 2020 le ciblage d'employés de l'ORGANISATION MONDIALE DE LA SANTÉ (OMS) et de l'entreprise pharmaceutique GILEAD SCIENCES INC par des attaquants liés à l'Iran au moyen de courriels de hameçonnage ciblés, sans toutefois être en mesure de confirmer des compromissions.

En juillet 2020, le NATIONAL CYBER SECURITY CENTRE du Royaume-Uni (NCSC-UK) a publié un rapport portant sur le ciblage et la compromission, au moyen des codes malveillants WellMess et WellMail, de plusieurs organisations liées au développement de vaccins contre la Covid-19 au Canada, au Royaume-Uni et aux États-Unis. Cette campagne a été associée par le NCSC-UK au mode opératoire APT29, réputé lié en source ouverte au service de renseignement extérieur russe, le SVR [44]. Selon le rapport, les opérateurs de ce MOA auraient exploité

des équipements vulnérables exposés sur Internet pour accéder aux systèmes de leurs victimes à des fins d'espionnage [45].

Le même mois, le DEPARTMENT OF JUSTICE des États-Unis a également mis en accusation deux ressortissants chinois pour leur rôle dans des opérations d'espionnage économique depuis 2014. Leur dernière opération avait notamment visé des centres de recherches sur la Covid-19 aux États-Unis. Les deux accusés auraient en effet recherché des vulnérabilités exploitables dans les réseaux d'entités de biotechnologies ou en lien avec la recherche de traitements contre la Covid-19, dont l'entreprise MODERNA [46, 47]. Le journal espagnol EL PAIS a également rapporté qu'au cours de l'année 2020, des attaquants informatiques associés à la Chine auraient exfiltré des données de centres de recherche médicale basés en Espagne [48].

En novembre 2020, l'éditeur de sécurité MICROSOFT a rapporté le ciblage d'entités liées à la recherche clinique, à la fabrication et aux essais de vaccins contre la Covid-19 par des attaquants liés à des États, dont les opérateurs des MOA réputés nord-coréens Diamond Sleet et Ruby Sleet[14]. Les opérateurs du MOA Diamond Sleet auraient notamment cherché à compromettre des cibles *via* l'envoi de courriels de hameçonnage imitant des offres d'emplois, et destinés à récolter des authentifiants. Les opérateurs du MOA Ruby Sleet auraient également diffusé des courriels de hameçonnage ciblés sur le thème de la Covid-19, en imitant des représentants de l'ORGANISATION MONDIALE DE LA SANTÉ [49]. En février 2021, le média sud-coréen DAILY NK a détaillé la création, en janvier 2021, du « Bureau 325 » par les autorités nord-coréennes, un nouveau groupe d'attaquants informatiques directement lié au dirigeant nord-coréen Kim Jong Un et notamment dédié à la récupération d'informations en lien avec la Covid-19 [50]. En outre, selon l'éditeur de sécurité MANDIANT, différents MOA réputés liés à la Corée du Nord auraient potentiellement été employés de façon simultanée pendant la crise sanitaire, en partageant de l'outillage et en ciblant des acteurs du secteur de la santé en lien avec la recherche de traitements contre la Covid-19 [51]. Le même éditeur a également rapporté que les opérateurs du MOA réputé nord-coréen APT45, auraient continué à cibler le secteur de la santé et en particulier la recherche médicale au cours de l'année 2023 [52].

5.2 Ciblage stratégique d'entités du secteur de la santé

Les entités du secteur de la santé peuvent également être ciblées dans le cadre de campagnes d'espionnage visant une multitude de secteurs. Ces campagnes, parfois menées de manière opportuniste, permettent aux attaquants d'obtenir des accès à des SI pouvant être utilisés ultérieurement pour mener d'autres opérations offensives.

Ainsi, selon l'éditeur de sécurité MANDIANT, entre janvier et mars 2020, les opérateurs du MOA réputé lié à la Chine APT41 auraient ciblé des entités de plusieurs secteurs dans le monde entier, dont des entités pharmaceutiques, pour obtenir des accès non-autorisés *via* l'exploitation de vulnérabilités affectant des équipements CITRIX (CVE-2019-19781), CISCO (CVE-2019-1653 et CVE-2019-1652) et MANAGEENGINE (CVE-2020-10189). Certaines entités auraient été compromises. MANDIANT estime que les opérateurs du MOA APT41 pourraient avoir cherché à cibler un sous-ensemble d'entités préalablement sélectionné [53].

Au début de l'année 2023, les opérateurs du MOA réputé nord-coréen Lazarus auraient compromis des entités du secteur des télécommunications et de la santé en Europe et aux États-Unis, *via* l'exploitation d'une vulnérabilité affectant la solution ServiceDesk de MANAGEENGINE (CVE-2022-47966). Cette vulnérabilité était utilisée par les attaquants pour obtenir des accès non au-

14. Les MOA Diamond Sleet et Ruby Sleet étaient respectivement anciennement connus sous les alias MICROSOFT Zinc et Cerium. Le MOA Diamond Sleet est également connu sous l'alias Lazarus.

torisés et délivrer les codes malveillants QuiteRAT et CollectionRAT. Ces codes malveillants permettaient notamment de collecter des informations sur les appareils compromis et d'exécuter du code à distance [54, 55].

Au cours de l'année 2023, l'éditeur de sécurité MICROSOFT a par ailleurs rapporté avoir observé des activités de pulvérisation de mots de passe ou *password spraying* contre des centaines d'entités dans le monde, dont des entités pharmaceutiques. L'éditeur a associé ces activités au MOA réputé iranien Peach Sandstorm. Une partie de ces entités aurait été ciblée de façon opportuniste selon l'éditeur, étant donné le volume d'activités observé et la diversité des secteurs concernés [56].

6 MENACE À FINALITÉ DE DÉSTABILISATION

Les attaques informatiques à finalité de déstabilisation observées contre le secteur de la santé émanent notamment de groupes hacktivistes et peuvent prendre la forme d'attaques par déni de service distribué (DDoS), de défigurations de sites web et d'exfiltrations de données à des fins de divulgation.

Le ciblage du secteur de la santé s'inscrit le plus souvent dans des campagnes de déstabilisation plus larges en lien avec des sujets majeurs de l'actualité nationale ou internationale tels que l'offensive russe en Ukraine depuis février 2022 ou la guerre entre Israël et le Hamas depuis octobre 2023. Ces sujets agissent comme des catalyseurs de la menace hacktiviste.

Au cours de la crise sanitaire liée à la Covid-19, certaines entités du secteur de la santé ont toutefois été spécifiquement ciblées par des groupes hacktivistes visant à dénoncer des problématiques d'ordre sanitaire telles que la mauvaise gestion de la pandémie par certains gouvernements.

Les attaques informatiques conduites par des groupes hacktivistes visent essentiellement à attirer l'attention pour générer des effets psychologiques et ont des conséquences généralement limitées. Certaines attaques informatiques, telles que les attaques par DDoS, peuvent toutefois avoir un potentiel de déstabilisation plus important lorsqu'elles perturbent certains services de santé contraints par un fort besoin de continuité opérationnelle. Par exemple, lorsqu'elles visent des plateformes et des sites web, elles peuvent nuire à l'accès à l'information, à des données de santé ou encore à des services et ressources en ligne destinés aux patients.

Par ailleurs, des attaques informatiques à des fins de déstabilisation peuvent également être menées par des opérateurs potentiellement soutenus par des États.

6.1 Attaques par déni de service distribué

6.1.1 Attaques ciblant la France

En juin 2023, les sites Internet de plusieurs hôpitaux français dont celui de l'ASSISTANCE PUBLIQUE-HÔPITAUX DE PARIS ont été touchés par une attaque par DDoS qui a entrainé leur indisponibilité pendant plusieurs heures. Cette attaque a été revendiquée sur le réseau social Telegram par le groupe hacktiviste Anonymous Sudan [15] en réponse à la mort de Nahel Merzouk, adolescent tué par un policier dans la ville de Nanterre en France, le 27 juin 2023 [57].

Plus récemment, suite à l'arrestation de Pavel Durov, fondateur du service de messagerie TELEGRAM, le 25 août 2024 en France, de nombreux groupes hacktivistes pro-russes parmi lesquels le groupe Cyber Army of Russia Reborn ont revendiqué des attaques par DDoS contre des sites web d'entités françaises de secteurs variés, dont le site web de l'AGENCE NATIONALE DE SÉCURITÉ DES MÉDICAMENTS [58].

6.1.2 Attaques à l'étranger

En juillet 2022, le groupe hacktiviste pro-iranien Al-Tahira a revendiqué une attaque par DDoS contre le site web du ministère de la Santé israélien. Cette attaque informatique aurait été menée

15. Anonymous Sudan est un groupe hacktiviste apparu sur le réseau social Telegram le 19 janvier 2023, qui se revendique d'origine soudanaise, et qui semble entretenir des liens avec la sphère hacktiviste pro-russe.

en représailles aux bombardements dans la bande de Gaza par l'armée israélienne, à l'absence présumée de livraison de traitements contre la Covid-19, et au soutien d'Israël à l'Ukraine [59].

Entre décembre 2022 et mars 2023, une alliance de plusieurs groupes hacktivistes pro-russes menée par le groupe Killnet a conduit des attaques par DDoS contre plusieurs entités du secteur de la santé aux États-Unis et dans des pays de l'Organisation du Traité de l'Atlantique Nord en représailles au soutien apporté par ces pays à l'Ukraine [60].

6.2 Exfiltration de données à des fins de divulgation publique

En mai 2020, un groupe hacktiviste présumé brésilien nommé DigitalSp4ce aurait divulgué les résultats médicaux de l'ancien président brésilien Jair Bolsonaro, pour dénoncer la réponse du gouvernement brésilien face à la crise sanitaire. Ces données médicales auraient été dérobées dans une base de données d'un hôpital militaire. Le groupe hacktiviste a par ailleurs remis en question la validité des tests de dépistage du Covid-19 effectués par Jair Bolsonaro [61, 62].

En décembre 2020, l'Agence Européenne du Médicament aurait été victime d'une fuite de données. Ces données auraient été modifiées, puis mises à disposition gratuitement sur des forums cybercriminels. Les documents auraient été altérés à des fins de désinformation, vraisemblablement pour miner la confiance accordée au vaccin Pfizer-BioNTech [63, 64]. Cette compromission est survenue dans un contexte où l'Agence Européenne du Médicament devait valider le recours en Europe au vaccin développé par Pfizer-BioNTech contre la Covid-19 [65]. Le journal néérlandais De Volskrant a associé cet incident à des opérateurs potentiellement russes. Le même journal a par ailleurs expliqué que les attaquants auraient exploité une limite du mécanisme de double authentification pour compromettre les systèmes informatiques de l'Agence Européenne du Médicament et mener des activités d'espionnage, notamment en lien avec la stratégie vaccinale européenne et les vaccins achetés par différents pays [64].

Mi-octobre 2023, un groupe hacktiviste présumé indonésien nommé Infinite Insight aurait publié des données de près de 790 000 médecins aux États-Unis, potentiellement en réaction à l'assistance des États-Unis envers Israël et en soutien à la cause palestinienne [66].

6.3 Attaques informatiques à visée de sabotage

Les entités du secteur de la santé peuvent également être la cible d'attaques informatiques à des fins de sabotage, s'appuyant notamment sur l'usage de faux rançongiciels.

Ainsi, au cours de l'année 2021, plusieurs MOA réputés liés à l'Iran, dont les noms n'ont pas été précisés, ont été associés par des agences américaines et australiennes au ciblage d'une variété de secteurs aux États-Unis et en Australie, dont la santé, pour obtenir des accès non autorisés *via* l'exploitation de vulnérabilités affectant des équipements Fortinet et Microsoft Exchange [67]. Ces compromissions ont parfois abouti à des déploiements de rançongiciels. En juin 2021, une attaque par rançongiciel visant le Boston Children's Hospital aux États-Unis a été contrecarrée par les autorités et attribuée par le FBI à la République islamique d'Iran [68]. Un communiqué de presse du Département du Trésor américain publié en septembre 2022 associe entre autres cette attaque au MOA réputé iranien Nemesis Kitten [69].

7 RECOMMANDATIONS

Les recommandations suivantes sont principalement destinées aux prestataires de soins, qui constituent une des quatre catégories d'acteurs traités dans cet état de la menace. Elles visent à éclairer ces entités en matière de bonnes pratiques de cybersécurité à adopter afin de se prémunir contre les menaces détaillées précédemment. Ces mesures ne sont pas exhaustives, ne se substituent pas aux réglementations spécifiques qui peuvent concerner certaines entités, et doivent être adaptées et complétées dans le cadre du contexte opérationnel et fonctionnel du système d'information considéré.

Ainsi, afin de faire face aux menaces mises en lumière précédemment, l'ANSSI rappelle tout d'abord l'importance d'avoir une approche globable de la sécurité, en identifiant pour chaque entité :

- les actifs devant être protégés ;
- l'état actuel du système d'information les soutenant et du niveau de compétence des personnes l'utilisant ou l'opérant ;
- la nature des menaces vis-à-vis desquelles il convient de se préparer ;
- les risques et la priorisation des actions de sécurisation à mener ;
- les mesures de sécurité appropriées devant être mises en œuvre et entretenues dans le temps.

L'ANSSI rappelle également l'importance, notamment pour les établissements de santé, d'intégrer le RSSI dans l'ensemble des projets avec une dimension IT et d'encourager la collaboration entre le personnel de cybersécurité, le personnel IT et les ingénieurs biomédicaux afin de solidifier la connaissance sur les SI utilisés, faciliter leur sécurisation et une réponse efficace en cas d'incident informatique.

En outre, la mise en œuvre des recommandations du présent document doit s'appuyer sur une démarche itérative d'amélioration continue, traitant en priorité les risques les plus élevés de l'entité. Il est recommandé de se focaliser dans un premier temps sur l'état des lieux de son SI, la sensibilisation des ressources humaines et sur les mécanismes de résilience avant d'aborder la mise en œuvre des mesures de protection et de défense pour une meilleure maitrise des risques.

Dans cette section, les mesures de sécurité portent sur les thématiques suivantes :

- la sécurité des ressources humaines ;
- la gestion des risques ;
- l'acquisition, le développement et la maintenance ;
- l'architecture ;
- la gestion des identités et des accès ;
- la gestion des vulnérabilités ;
- la journalisation et détection de sécurité ;
- la résilience du système d'information.

Ces recommandations sont, lorsque cela est applicable, accompagnées de références vers des guides de l'ANSSI ou des ressources de l'Agence du Numérique en Santé et du Club RSSI Santé pour approfondir les sujets abordés. Des publications complémentaires peuvent également être consultés [70, 71]. Pour les mesures portant spécifiquement sur la protection des données, l'entité doit se référer à la réglementation qui lui est applicable comme par exemple le Règlement Général sur la Protection des Données (RGPD) pour les données personnelles, ou encore les

dispositions du Code de la Santé Publique relatives à la protection des données de santé telles que l'article L1111-8.

En complément de ces recommandations, une attention particulière doit être portée aux annuaires *Active Directory*, éléments critiques du SI qui permettent la gestion centralisée des comptes, des ressources et des permissions. Utiliser le service ADS (voir cert.ssi.gouv.fr/scans) et appliquer les recommandations fournies par le service permet d'améliorer considérablement la sécurité des annuaires *Active Directory*.

Le CERT-FR offre également un service de veille sur les vulnérabilités, qui permet d'être alerté sur les vulnérabilités critiques et d'obtenir des recommandations et mesures de contournement associées (cert.ssi.gouv.fr). En outre, le CERT santé met à disposition un service de cybersurveillance (https://cyberveille.esante.gouv.fr/les-services.

7.1 Sécurité des ressources humaines

R1

Sensibiliser les collaborateurs

Des sessions de sensibilisation doivent être organisées régulièrement afin de sensibiliser les utilisateurs et responsabiliser les administrateurs du système d'information. Les objectifs majeurs sont de mettre l'accent sur les enjeux de cybersécurité et de transmettre les bonnes pratiques à adopter face à une situation de cybermalveillance.

Pour les utilisateurs et administrateurs du système d'information (SI), communiquer les précautions suivantes :

- ne pas ouvrir les messages dont la provenance ou la forme est inconnue ou suspecte, car il pourrait s'agir d'un contenu malveillant (par exemple : un rançongiciel) ;
- se méfier des extensions de pièces jointes douteuses (par exemple : .pif ; .com ; .bat ; .exe ; .vbs ; .lnk…), et qui peuvent contenir des codes malveillants ;
- adopter de bonnes pratiques de navigation sur Internet (vérifier l'authenticité d'un site Web avant de communiquer des authentifiants, ne télécharger de logiciels que depuis le site de leur éditeur) ;
- ne pas connecter sur son poste de travail un support USB trouvé par hasard, car celui-ci pourrait contenir un logiciel malveillant.

Pour les administrateurs de SI, il est important d'axer la communication autour des thèmes suivants :

- les administrateurs représentent des cibles privilégiés pour les attaquants de par la nature de leurs missions, leurs accès et les secrets d'authentification dont ils disposent ;
- les administrateurs doivent protéger les moyens techniques mis à leur disposition avec un niveau de vigilance et de sécurité supplémentaire par rapport aux utilisateurs.

7.2 Gestion des risques

R2

Réaliser une cartographie de son SI et de son environnement

Tous les éléments constitutifs du système d'information doivent être recensés dans un document de cartographie afin d'obtenir une meilleure lisibilité et contrôle du système d'information. La cartographie doit permettre de répondre à des enjeux variés :

- **d'écosystème**, à travers l'identification de l'ensemble des parties prenantes avec lesquelles le SI interagit pour remplir sa fonction et notamment les prestataires de services ;
- **métier**, à travers l'identification des processus métiers et informations essentiels du SI. Une attention particulière doit être portée à l'inventaire des données sensibles (données personnelles, de santé, ou stratégiques liées au savoir-faire de l'entité, à des informations comptables, etc.) ;
- **physique**, à travers l'identification des composants physiques du SI qui soutiennent les processus et informations essentiels ainsi que leur localisation géographique (permettant par exemple d'identifier où les données sensibles sont hébergées) ;
- **logique** à travers l'identification de la segmentation logique du réseau et des liens logiques entre ses segments. Cela inclut notamment la segmentation du réseau au niveau 2 du modèle OSI (ex. VLAN) et au niveau 3 du modèle OSI (ex. découpe de l'adressage IP) ainsi que les équipements réseaux et de sécurité permettant l'interconnexion de ces segments (ex. routage, filtrage, etc.) ;
- **applicatif**, à travers l'identification des composants logiciels du système qui soutiennent les processus et informations essentiels du SI. En particulier, les échanges d'informations au travers du réseau entre ces composants doivent être identifiés dans une matrice de flux.

Il est important de noter que la constitution d'une cartographie est un processus itératif et que l'entité doit adapter la granularité de sa cartographie à l'outillage dont elle dispose et à sa capacité à la maintenir dans le temps. Ce document et ses annexes doivent rester avant tout une aide à la prise de décision dans la maitrise de ses risques ou en cas d'incident.

Pour aller plus loin : ANSSI, *Cartographie du système d'information*, 21 novembre 2018 [72].

R3

Mener une analyse de risque

Une analyse de risque doit être réalisée et maintenue à jour régulièrement (par exemple annuellement) ou en cas d'évolution notable de la menace ou du contexte en prenant en compte l'ensemble des dépendances et prestataires sur lesquels s'appuie l'entité.

Cette analyse de risque doit notamment mettre en exergue les risques numériques que ces entités externes feraient peser sur l'organisation tant sur le plan technique qu'organisationnel, ainsi que les impacts sur le secret professionnel ou tout autre secret en lien avec les activités de l'entité. Ainsi, dans le cadre de l'utilisation d'un service numérique (échange de fichiers, messagerie, etc.), il convient de systématiquement s'interroger sur le niveau de confiance à accorder à ce service, dans l'optique de protéger les informations traitées au bon niveau. Cette évaluation du niveau de confiance à accorder à un service externe doit s'appuyer notamment sur l'origine du fournisseur du service, la localisation du service (en prenant en compte le contexte géopolitique du moment) ou encore son niveau de sécurisation (disponibilité, intégrité, confidentialité, traçabilité).

Il est donc important pour la maitrise des risques de l'entité d'identifier des mesures de sécurité à exporter vers ces entités externes en plus des mesures de sécurité portant sur la cible de l'étude.

Pour aller plus loin : ANSSI, *La méthode EBIOS Risk Manager*, 18 juillet 2022 [73].

7.3 Acquisition, développement et maintenance

R4

Inclure des exigences de sécurité dans les cahiers des charges

Dès la conception de projets internes, et lors de l'établissement de contrats de sous-traitance ou d'achat de logiciels, des exigences de cybersécurité issues de référentiels normatifs et de l'analyse de risque doivent être incluses dans les cahiers des charges. Ces exigences doivent notamment couvrir les objectifs de sécurité :

- **sur la protection des données hébergées jugées sensibles** ;
- **sur les choix techniques**, déclinés en exigences dans les documents de spécification : fourniture de documentation (utilisateur, maintenance et de configuration sécurisée), redondance afin de permettre la maintenance, etc. ;
- **sur le maintien en condition de sécurité et en condition opérationnelle des logiciels et de leurs dépendances** (**système d'exploitation, bibliothèques tierces, etc.**) : fourniture des correctifs de sécurité pendant une période donnée, notification d'obsolescence logicielle, etc. ;

Dans le cas des contrats de prestation, une attention sera portée à la définition **des objectifs de sécurité des équipements propres au sous-traitant, de ses éventuels moyens d'accès distants, ainsi que ses droits d'accès délégués dans le système d'information**. Afin d'évaluer le niveau de conformité du soumissionnaire, un plan d'assurance sécurité (PAS) doit lui être demandé en réponse au cahier des charges. Ses engagements peuvent être audités en cours de prestation en accord avec les conventions d'audit établis au titre du marché.

Par exemple, il pourra être demandé :

- d'utiliser un client VPN par certificat (ou à défaut par mot de passe, accessible uniquement depuis ses adresses IP) ;
- d'utiliser un poste géré par l'entreprise prestataire, bénéficiant d'une supervision de sécurité, et de fournir la politique de sécurité qui s'y applique ;
- de fournir une matrice des flux réseau nécessaires, afin de n'autoriser que ces flux ;
- de fournir une liste des délégations nécessaires dans le système d'information, afin de fournir un compte n'ayant que ces droits.

Pour aller plus loin :

- ANSSI, *Externalisation et sécurité des systèmes d'information : un guide pour maitriser les risques*, 12 mars 2010 [74]
- Club RSSI Santé, *Clausier sécurité 2024*, mai 2024 [75]

7.4 Architecture

R5

Mettre en œuvre une passerelle d'interconnexion à Internet

Une passerelle d'interconnexion à Internet doit être mise en œuvre afin de protéger le SI interne des menaces provenant du réseau Internet. Cette passerelle doit :

- être incontournable pour les flux entrants et sortants du système d'information ;
- constituer des zones démilitarisées (DMZ) pour les éventuels systèmes de moindre confiance (par exemple, des serveurs exposés à Internet, ou obsolètes) ;
- si des accès distants sont nécessaires, imposer la mise en œuvre d'un VPN avec authentification par certificat (ou à défaut, par mot de passe et deuxième facteur).

Pour aller plus loin : ANSSI, *Recommandations relatives à l'interconnexion d'un système d'information à Internet*, 19 juin 2020 [76]

R6

Cloisonner et filtrer les différents systèmes d'information

L'ensemble des systèmes de l'entité doit être cloisonné de manière logique *a minima* (par exemple par VLAN au niveau réseau, par VM au niveau des équipements, etc.) afin d'éviter la propagation et la latéralisation d'une attaque sur l'ensemble des processus métiers de l'entité. Les interconnexions entre les différents SI doivent être contrôlées par des dispositifs de filtrage autorisant uniquement les flux nécessaires au bon fonctionnement des activités de l'entité. Les SI à cloisonner sont par exemple :

- le SI bureautique ;
- le SI de gestion des dispositifs biomédicaux pour les prestataires de soins ;
- le SI de service d'urgence pour les établissements de santé ;
- le SI de Gestion Technique du Bâtiment (GTB)/Gestion Technique Centralisée (GTC) ;
- le SI d'administration.

Pour aller plus loin spécifiquement sur le cloisonnement de l'administration : ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, 11 mai 2021 [77]

R7

Protéger les données par mécanisme cryptographique

Les données du SI transitant sur un réseau tiers ou ayant un fort besoin en confidentialité doivent être protégées en confidentialité par l'utilisation de mécanismes cryptographiques conformes à l'état de l'art. Cela concerne plus particulièrement :

- toute donnée transitant sur un réseau tiers ;
- les données d'administration transitant sur tout réseau interne ou tiers ;
- les données sensibles (données de santé, données personnelles, etc.) transitant sur tout réseau interne ou tiers ;
- les données sensibles (données de santé, données personnelles, etc.) au repos en cas d'hébergement chez un prestataire ou fournisseur de services nuagiques ;
- les données sensibles stockées sur des supports amovibles (clé USB, disque dur portable).

7.5 Gestion des identités et des accès

R8

Identification unique des utilisateurs

Tous les accès des utilisateurs aux ressources du SI de l'entité doivent être identifiés de manière unique. Les comptes uniques doivent être centralisés afin d'en faciliter la gestion. Cependant ce type de solution (et notamment Microsoft Active Directory) peut également créer un point de vulnérabilité unique et doit donc être configurée avec soin et faire l'objet d'audits réguliers.

Pour aller plus loin : ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory*, 18 octobre 2023 [78]

R9

Protéger les données d'authentification

Les données d'authentification permettant de prouver l'identité d'un utilisateur avant tout accès à une ressource du SI doivent être protégées avec notamment :

- l'utilisation d'un mot de passe fort bien mémorisé par les utilisateurs sans nécessiter un renouvellement à intervalles courts ;
- la limitation du nombre de tentatives d'authentification sur une période de temps donnée, afin de réduire les probabilités d'authentification frauduleuses en ligne par force brute ;
- pour l'authentification vers des services distants, la migration vers des méthodes permettant de prouver son identité sans fournir de secret. Par exemple, on remplacera l'authentification consistant à envoyer son mot de passe aux équipements réseau et systèmes Unix par une authentification SSH par clé publique. Les applications Web demandant un nom d'utilisateur et un mot de passe peuvent parfois être configurées pour utiliser l'authentification Kerberos automatique sous Unix et Windows, ou à défaut l'authentification mutuelle par certificat TLS. Les applications incompatibles peuvent parfois être placées derrière un serveur mandataire inverse (*reverse proxy*) remplissant ces tâches à leur place ;
- pour les services non compatibles avec le point ci-dessus, l'utilisation d'un coffre-fort de mots de passe permettant l'utilisation de secrets d'authentification distincts pour accéder à différents services en limitant le nombre d'authentifiants à retenir.

Les applications hébergeant des données sensibles et les services exposés à Internet (les VPN en particulier) doivent être protégés par une authentification forte, non vulnérable aux attaques d'hameçonnage. Par exemple, privilégier l'authentification par certificats clients aux mots de passe, ou à défaut imposer un deuxième facteur comme un *One-Time Password*.

Pour aller plus loin : ANSSI, *Recommandations relatives à l'authentification multifacteurs et aux mots de passe*, 8 octobre 2021 [79]

R10

Limiter les droits d'accès aux ressources du SI

Le principe de moindre privilège doit être appliqué pour tout accès des utilisateurs et administrateurs aux ressources du SI en s'assurant notamment que :

- les utilisateurs ne sont pas administrateurs de leur poste de travail. Ainsi, la configuration des postes reste homogène, et les logiciels installés peuvent être inventoriés et suivis pour leurs mises à jour. De plus, les éventuels codes malveillants exécutés auront des conséquences limitées ;
- les comptes d'administration sur les ressources du système d'information sont limités au strict nécessaire et que des postes d'administration non connectés à Internet sont utilisés. En effet, lors d'une compromission, on constate que les attaquants s'emploient souvent à accéder à ces comptes privilégiés.

Pour aller plus loin sur la gestion des comptes à privilèges : ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, 11 mai 2021 [77]

R11

Limiter les droits d'accès aux données sensibles

Une politique d'accès adaptée aux différentes données de l'entité doit être mise en œuvre selon le principe du moindre privilège. L'objectif est de réduire l'accès aux données identifiées comme sensibles et de limiter les fuites d'informations traitées au sein de l'entité (par exemple les données personnelles, les données de santé, les données de recherche ou liées au savoir-faire de l'entité, etc.).

En particulier, chaque entité doit s'attacher à :

- identifier parmi ses traitements de données, les informations sensibles à protéger au regard de la réglementation applicable et du risque d'atteinte à la confidentialité ;
- adopter un marquage approprié de ses données selon leur classification : l'objectif du marquage est d'apporter la connaissance du niveau de sensibilité des informations à toute personne les manipulant. Dans le cas de fichiers informatiques par exemple, le marquage doit également figurer sur le nom du fichier et du répertoire de stockage.

7.6 Gestion des vulnérabilités

R12

Durcir la configuration des équipements

Un durcissement de la configuration des équipements du SI doit être réalisé afin d'en limiter la surface d'attaque. Au niveau matériel, il convient de rendre l'authentification obligatoire pour modifier le paramétrage du BIOS et le chiffrement des disques lorsque l'équipement le permet. Au niveau logiciel (OS et applications), il convient de supprimer ou désactiver les services inutiles afin de faciliter le maintien en condition de sécurité, de supprimer les comptes et authentifiants par défaut, et d'activer des fonctions de filtrage local à l'équipement.

R13

Maintenir à jour le système d'information

Une politique de maintien en condition opérationnelle (MCO) et de maintien en condition de sécurité (MCS) doit être définie et mise en œuvre afin de renforcer la sécurité et la stabilité de tous les SI de l'entité. Les logiciels doivent être dans des versions maintenues par les éditeurs et les correctifs de sécurité appliqués en priorité sur les équipements et services directement exposés sur Internet (par exemple, le pare-feu périmétrique, les postes utilisateurs avec accès à Internet etc.), sachant qu'ils sont particulièrement exposés aux attaques cyber. À noter que pour chaque nouveau projet, des exigences de MCO et le MCS doivent être systématiquement intégrées dans les cahiers des charges.

7.7 Journalisation et Détection de Sécurité

R14

Utiliser une solution de protection contre les logiciels malveillants

Une solution de protection contre les logiciels malveillants doit être mise en œuvre lorsque cela est possible sur les systèmes ayant accès à ou traitant du contenu en provenance d'Internet (par exemple les postes de travail ou les serveurs relais de messagerie en DMZ).
Ces outils ne garantissent pas une protection contre des logiciels malveillants inconnus mais peuvent, dans certains cas, empêcher une compromission.

Pour aller plus loin : CERT Santé, *Du bon usage d'un EDR*, 22 juin 2023 [80]

R15

Centraliser les journaux d'évènements et les alertes des capteurs de sécurité

Les journaux d'évènements (des composants, des systèmes d'exploitation, des applications, etc.) ainsi que les alertes de sécurité générées par des capteurs de sécurité (par exemple, par la solution de protection contre les logiciels malveillants) doivent être activés et centralisés. Cela permet d'investiguer les incidents de sécurité *post-mortem*, voire de détecter un incident de sécurité avant que l'attaquant ne parvienne à réaliser son objectif. La centralisation des évènements de sécurité contribue d'une part à sécuriser la collecte des évènements et d'autre part à faciliter les opérations de détection et d'analyse en cas d'incident.

Il convient en particulier de :

- identifier les scénarios de menaces à détecter incluant notamment les menaces du présent document (rançongiciel, etc.) ;
- activer et centraliser les évènements utiles aux objectifs de détection les plus critiques dans la limite des capacités de l'entité à traiter les évènements sous 24 heures ;
- améliorer de manière itérative la capacité de traitement des évènements par l'entité afin de couvrir l'ensemble des scénarios de menaces à détecter.

Pour aller plus loin :

- ANSSI, *Recommandations de sécurité pour l'architecture d'un système de journalisation*, 28 janvier 2022 [81]
- ANSSI, *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory*, 28 janvier 2022 [82]

R16

Maintenir à jour les règles de détection

Les règles de détection du système de supervision de sécurité (par exemple, la base de signatures d'un logiciel antivirus) doivent être maintenues à jour pour prendre en compte l'évolution du SI et des menaces afin de s'assurer régulièrement

de l'absence de logiciel malveillant connu sur les espaces de stockage des fichiers de l'entité.

7.8 Résilience du système d'information

R17

Définir un PRA et un PCA

L'entité doit mettre en œuvre les moyens techniques et humains lui permettant, suite à un incident de sécurité, de maintenir ses activités ou ses services dans un mode dégradé et de faciliter le retour à la normale. Ces éléments doivent être formalisés au travers d'un Plan de Continuité d'Activité (PCA) et d'un Plan de Reprise d'Activité (PRA) couvrant les menaces d'origine accidentelle mais aussi les menaces d'origine malveillante avec notamment :

- les **attaques par rançongiciels** qui peuvent affecter la disponibilité des systèmes et/ou les données de l'entité ;
- les **exfiltrations de données** qui peuvent nuire à la disponibilité et la confidentialité des données de l'entité ;
- les **attaques affectant les fournisseurs de biens ou services** avec lesquels le ou les SI de l'entité ont une forte dépendance (par exemple, l'indisponibilité de services en SaaS fournis par un prestataire informatique, etc.) ;
- les **attaques par DDoS** qui peuvent affecter la disponibilité des ressources exposées à Internet (sites web, etc.).

Des procédures dégradées permettant aux services essentiels d'être rendus en dépendant le moins possible du système d'information pourront par exemple être définies. Ces procédures peuvent être améliorées de façon itérative en les testant régulièrement (par exemple, tous les deux mois). Ces tests sont également nécessaires pour fournir aux administrateurs du système d'information des périodes de maintenance durant lesquelles effectuer les mises à jour et les changements de configuration nécessaires.

Pour aller plus loin : Kits de l'Agence du Numérique en Santé, *Cybersécurité accélération et Résilience des Etablissements (CaRE) - Gouvernance et Résilience*, 2024 [83]

R18

Assurer la sauvegarde des données

Une politique de sauvegarde régulièrement mise à jour doit être définie, appliquée et testée afin de pallier la corruption ou l'indisponibilité de données dues à un incident ou une compromission (par exemple, liés à un rançongiciel). Pour les éléments les plus critiques, une sauvegarde hors ligne doit être prévue afin de garantir une restauration en cas d'attaque par un rançongiciel. En fonction du niveau de sensibilité des données, les sauvegardes doivent être chiffrées afin d'en garantir la confidentialité.

Il convient en particulier de :

- définir une liste des données et services vitaux pour l'organisme et les ser-

veurs concernés ;
- définir la fréquence des sauvegardes ;
- réaliser des sauvegardes des données critiques et prévoir au minimum une sauvegarde hors ligne (à intervalle régulier) afin de se prémunir des attaques de type rançongiciel ;
- rédiger et tester régulièrement les procédures de restauration ;
- rédiger et tester les procédures d'administration et d'exécution des sauvegardes ;
- définir des restrictions d'accès aux sauvegardes.

Pour aller plus loin : ANSSI, *Sauvegarde des systèmes d'information*, 25 octobre 2024 [84]

R19

Mettre en œuvre un plan de réponse aux cyberattaques

L'entité doit être préparée à la gestion d'une crise cyber pour assurer une réaction rapide et adaptée en cas d'attaque informatique réelle.

Il convient en particulier de :
- prévoir une organisation et des procédures de gestion de crise ;
- consolider un cahier de gestion de crise avec les coordonnées de l'ensemble des acteurs utiles, dont notamment le CERT Santé ;
- identifier et préparer les équipes aux premières actions d'urgence et conservatoires pour protéger *a minima* le service et restreindre les activités malveillantes ;
- réaliser des exercices de gestion de crise.

Les exercices de gestion de crise sont particulièrement importants et ne doivent pas être négligés. Ils permettent de démontrer l'efficacité du dispositif de gestion de crise mis en œuvre et l'appropriation par les équipes des procédures et des réflexes à avoir en cas d'incident avéré.

Pour aller plus loin :
- ANSSI, *Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique*, 6 décembre 2021 [85]
- ANSSI, *Organiser un exercice de gestion de crise cyber*, 14 octobre 2020 [86]
- Kits de l'Agence du Numérique en Santé, *Cybersécurité accélération et Résilience des Etablissements (CaRE) - Gouvernance et Résilience*, 2024 [83]

8 Références

[1] Proofpoint et Ponemon Institute. *Cyber Insecurity in Healthcare : The Cost and Impact on Patient Safety and Care*. 11 mai 2023.
URL : https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf.

[2] Agence du Numérique en Santé. *Cybersécurité accélération et Résilience des Établissements (CaRE). Le plan d'action pour protéger nos établissements face à la menace cyber.* 31 décembre 2023.
URL : https://esante.gouv.fr/sites/default/files/media_entity/documents/doc-programme-care-231214-20h_pap%5B17%5D.pdf.

[3] ANSSI. *Les parcours de cybersécurité : rapport d'activité 2023. Volet cybersécurité de France Relance*. 31 mars 2024.
URL : https://cyber.gouv.fr/sites/default/files/document/les_parcoursde_cybersecurite_rapport_d_activite_2023.pdf.

[4] Haute Autorité de Santé. *Certification des établissements de santé. Ajustements 2024 du référentiel & témoignages d'établissements.* 12 septembre 2023.
URL : https://www.has-sante.fr/upload/docs/application/pdf/2023-09/ajustements_du_referentiel_2024_et_temoignages_detablissement_-_diaporama.pdf.

[5] Medtronic. *Urgent Medical Device Correction*. 20 septembre 2022.
URL : https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice19-letter.

[6] Federal Bureau of Investigation. *Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities*. 12 septembre 2022.
URL : https://www.aha.org/system/files/media/file/2022/09/fbi-pin-tlp-white-unpatched-and-outdated-medical-devices-provide-cyber-attack-opportunities-sept-12-2022.pdf.

[7] Armis. *Nine Vulnerabilities in Critical Infrastructure Used by 80% of Major Hospitals in North America*. 2 août 2021.
URL : https://www.armis.com/research/pwnedpiper/.

[8] Swisslog Healthcare. *Statement : TransLogic Firmware Vulnerabilities*. 30 juillet 2021.
URL : https://www.swisslog-healthcare.com/-/media/swisslog-healthcare/documents/company/news/2021/statement-translogic-firmware-vulnerability.pdf?rev=3bb0280844a64cb7967ac75hash=AF65CC76A0BE4F44EBBB1C42EDEB346C.

[9] ENISA. *Health Threat Landscape*. 5 juillet 2023.
URL : https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] University of Minnesota. *Hacked to Pieces ? The Effects of Ransomware Attacks on Hospitals and Patients*. 4 octobre 2023.
URL : https://papers.ssrn.com/abstract=4579292.

[11] CISA. *North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector*. 6 juillet 2022.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a#:~:text=The%20Federal%20Bureau%20of%20Investigation,sponsored%20cyber%20actors%20since%20at.

[12] CISA. *Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities*. 9 février 2023.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a.

[13] US Department of Justice. *North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers*. 25 juillet 2024.
URL : https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

[14] ANSSI. *FIN12. Un groupe cybercriminel aux multiples rançongiciels*. 18 septembre 2023.
URL : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf.

[15] Le Monde. *Cyberattaque contre l'hôpital de Corbeil-Essonnes : ce que l'on sait sur les données diffusées*. 26 septembre 2022.
URL : https://www.lemonde.fr/pixels/article/2022/09/26/apres-la-cyberattaque-contre-l-hopital-de-corbeil-essonnes-ce-que-l-on-sait-sur-les-donnees-diffusees_6143245_4408996.html.

[16] Le Parisien. *Corbeil-Essonnes : rançon, patients réorientés... Ce que l'on sait de la cyberattaque qui paralyse l'hôpital sud-francilien*. 22 août 2022.
URL : https://www.leparisien.fr/essonne-91/corbeil-essonnes-lhopital-du-chsf-victime-dun-piratage-informatique-une-rancon-demandee-22-08-2022-JIXPBOTJQJDJTKKW3QD6WZEQJI.php.

[17] France Culture. *Cyberattaques - Les pieds sur Terre*. 11 janvier 2023.
URL : https://www.radiofrance.fr/franceculture/podcasts/les-pieds-sur-terre/cyberattaques-7095850.

[18] The Record. *Seattle Cancer Center Confirms Cyberattack after Ransomware Gang Threats*. 15 décembre 2023.
URL : https://therecord.media/seattle-fred-hutch-cancer-center-ransomware-attack.

[19] Ascension. *Cybersecurity Event Update*. 9 mai 2024.
URL : https://about.ascension.org/cybersecurity-event.

[20] Bleeping Computer. *Ascension Redirects Ambulances after Suspected Ransomware Attack*. 10 mai 2024.
URL : https://www.bleepingcomputer.com/news/security/healthcare-giant-ascension-redirects-ambulances-after-suspected-Black-Basta-ransomware-attack/.

[21] NPR. *Cyberattack Led to Harrowing Lapses at Ascension Hospitals, Clinicians Say*. 19 juin 2024.
URL : https://www.npr.org/2024/06/19/nx-s1-5010219/ascension-hospital-ransomware-attack-care-lapses.

[22] Bleeping Computer. *Ascension Healthcare Takes Systems Offline after Cyberattack*. 8 mai 2024.
URL : https://www.bleepingcomputer.com/news/security/ascension-healthcare-takes-systems-offline-after-cyberattack/.

[23] ZDNet. *Après la cyberattaque, une facture de 7 millions d'euros pour l'hôpital de Corbeil-Essonnes*. 28 septembre 2022.
URL : https://www.zdnet.fr/actualites/apres-la-cyberattaque-une-facture-de-7-millions-d-euros-pour-l-hopital-de-corbeil-essonnes-39947792.htm.

[24] The Record. *Critical Incident Declared as Ransomware Attack Disrupts Multiple London Hospitals*. 4 juin 2024.
URL : https://therecord.media/london-hospitals-ransomware-attack-critical-incident-declared.

[25] Le Monde. *Près de 400 gigaoctets de données personnelles de patients britanniques publiées en ligne après un piratage*. 21 juin 2024.
URL : https://www.lemonde.fr/pixels/article/2024/06/21/pres-de-400-gigaoctets-de-donnees-personnelles-de-patients-britanniques-publiees-en-ligne-apres-un-piratage_6242026_4408996.html.

[26] Bleeping Computer. *London Hospitals Face Blood Shortage after Synnovis Ransomware Attack*. 10 juin 2024.
URL : https://www.bleepingcomputer.com/news/security/london-hospitals-face-blood-shortage-after-synnovis-ransomware-attack/.

[27] Becker's Health IT. *Hackers Lurked in Change Healthcare's Network for More than a Week*. 22 avril 2024.
URL : https://www.beckershospitalreview.com/cybersecurity/hackers-lurked-in-change-healthcares-network-for-more-than-a-week.html.

[28] Bleeping Computer. *UnitedHealth : Change Healthcare Cyberattack Caused $872 Million Loss*. 16 avril 2024.
URL : https://www.bleepingcomputer.com/news/security/unitedhealth-change-healthcare-cyberattack-caused-872-million-loss/.

[29] CyberScoop. *Notorious Ransomware Group Claims Responsibility for Attacks Roiling US Pharmacies*. 28 février 2024.
URL : https://cyberscoop.com/ransomware-alphv-healthcare-pharmacies/.

[30] Microsoft Threat Intelligence. *Storm-0978 Attacks Reveal Financial and Espionage Motives*. 11 juillet 2023.
URL : https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/.

[31] HackManac X Channel. *CyberAttack France : Ethypharm has been listed as a victim by the Underground Team ransomware group.* 2 juillet 2024.
URL : https://x.com/H4ckManac/status/1808005267495219376.

[32] Recorded Future. *The Business of Fraud : Sales of PII and PHI*. 17 février 2022.
URL : https://www.recordedfuture.com/blog/business-fraud-sales-pii-phi.

[33] Security Week. *Data Stolen From MediSecure for Sale on Dark Web*. 28 mai 2024.
URL : https://www.securityweek.com/data-stolen-from-medisecure-for-sale-on-dark-web/.

[34] ANSSI. *Exfiltration de données du secteur social : retour d'expérience du CERT-FR*. 18 septembre 2024.
URL : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-009.pdf.

[35] Le Monde. *Cyberattaque contre Viamedis et Almerys : quelles précautions prendre ?* 8 février 2024.
URL : https://www.lemonde.fr/pixels/article/2024/02/08/fuite-de-donnees-de-sante-du-tiers-payant-quelles-precautions-prendre_6215410_4408996.html.

[36] Recorded Future. *Threats to the Healthcare Sector Amid Global COVID-19 Pandemic*. 13 novembre 2020.

[37] ReliaQuest. *The Rise of Initial Access Brokers - ReliaQuest*. 22 février 2021.
URL : https://www.reliaquest.com/blog/rise-of-initial-access-brokers/.

[38] Le Parisien. *Ils avaient vendu près de 7000 faux passes sanitaires : un hacker et des revendeurs arrêtés*. 11 juillet 2022.
URL : https://www.leparisien.fr/faits-divers/ils-avaient-vendu-pres-de-7000-faux-passes-sanitaires-un-hacker-et-des-revendeurs-arretes-11-07-2022-6BQ6PTFOEVA2JIPQCEWFSS3QUI.php.

[39] U.S. Attorney's Office, Eastern District of Virginia. *Eastern District of Virginia : EDVA Seizes Seven Websites Used to Collect Personal Information and Illegally Profit from the COVID-19 Pandemic*. 26 mars 2021.
URL : https://www.justice.gov/usao-edva/pr/edva-seizes-seven-websites-used-collect-personal-information-and-illegally-profit-covid.

[40] La République de Seine et Marne. *Fontainebleau : les gendarmes démantèlent une vaste escroquerie à la carte bancaire*. 27 septembre 2023.
URL : https://actu.fr/ile-de-france/fontainebleau_77186/fontainebleau-les-gendarmes-demantelent-une-vaste-escroquerie-a-la-carte-bancaire_60135119.html.

[41] l'Assurance Maladie. *Attention aux appels, courriels et SMS frauduleux*. 1er février 2024.
URL : https://www.ameli.fr/assure/droits-demarches/principes/attention-appels-courriels-frauduleux.

[42] Federal Bureau of Investigation. *Cyber Criminals Targeting Healthcare Payment Processors, Costing Victims Millions in Losses*. 14 septembre 2022.
URL : https://www.ic3.gov/Media/News/2022/220914-2.pdf.

[43] Mandiant. *APT42 : Crooked Charms, Cons, and Compromises*. 12 août 2022.
URL : https://cloud.google.com/blog/topics/threat-intelligence/apt42-charms-cons-compromises.

[44] CISA. *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA*. 9 mai 2022.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.

[45] NCSC-UK. *Advisory : APT29 Targets COVID-19 Vaccine Development*. 16 juillet 2020.
URL : https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf.

[46] US Deparment of Justice. *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research*. 7 juillet 2020.
URL : https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

[47] Reuters. *Exclusive : China-backed Hackers 'Targeted COVID-19 Vaccine Firm Moderna'*. 31 juillet 2020.
URL : https://www.reuters.com/article/technology/exclusive-china-backed-hackers-targeted-covid-19-vaccine-firm-moderna-idUSKCN24V38H/.

[48] El País English. *Chinese Hackers Accused of Stealing Information from Spanish Centers Working on Covid-19 Vaccine*. 18 septembre 2020.
URL : https://english.elpais.com/society/2020-09-18/chinese-hackers-accused-of-stealing-information-from-spanish-centers-working-on-covid-19-vaccine.html.

[49] Microsoft. *Cyberattacks Targeting Health Care Must Stop*. 13 novembre 2020.
URL : https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/.

[50] Daily NK. *Kim Jong Un Is Directly Handling Results of New COVID-19 Hacking Organization's Work*. 5 février 2021.
URL : https://www.dailynk.com/english/kim-jong-un-directly-handling-results-new-covid-19-hacking-organization-work/.

[51] Mandiant. *Assessed Cyber Structure and Alignments of North Korea in 2023*. 10 octobre 2023.
URL : https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023.

[52] Mandiant. *APT45 : North Korea's Digital Military Machine*. 25 juillet 2024.
URL : https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine.

[53] Mandiant. *APT41 Initiates Intrusion Campaign Using Multiple Exploits*. 25 mars 2020.
URL : https://cloud.google.com/blog/topics/threat-intelligence/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.

[54] Cisco Talos. *Lazarus Group Exploits ManageEngine Vulnerability to Deploy QuiteRAT*. 24 août 2023.
URL : https://blog.talosintelligence.com/lazarus-quiterat/.

[55] Cisco Talos. *Lazarus Group's Infrastructure Reuse Leads to Discovery of New Malware*. 24 août 2023.
URL : https://blog.talosintelligence.com/lazarus-collectionrat/.

[56] Microsoft Security Blog. *Peach Sandstorm Password Spray Campaigns Enable Intelligence Collection at High-Value Targets*. 14 septembre 2023.
URL : https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/.

[57] BFMTV. *Des sites web d'hôpitaux français inaccessibles, des hackers revendiquent une cyberattaque*. 30 juin 2023.
URL : https://www.bfmtv.com/tech/cybersecurite/plusieurs-hopitaux-francais-vises-par-une-cyberattaque_AV-202306300489.html.

[58] Le Parisien. *Arrestation de Pavel Durov : vague de cyberattaques et réactions publiques en soutien au patron de Telegram*. 25 août 2024.
URL : https://www.leparisien.fr/faits-divers/arrestation-de-pavel-durov-vague-de-cyberattaques-et-declarations-publiques-en-soutien-au-patron-de-telegram-25-08-2024-5J7DD64YGBFK7MWXBPTLJF3QG4.php.

[59] Ynetnews. *Health Ministry Website down after Iranian Cyberattack*. 17 juillet 2022.
URL : https://www.ynetnews.com/business/article/hynaba11h5.

[60] Health Sector Cybersecurity Coordination Center. *KillNet's Targeting of the Health and Public Health Sector*. 5 avril 2023.
URL : https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf.

[61] TecMundo. *Hackers invadem hospital e não encontram exame para covid-19 de Bolsonaro*. 14 mai 2020.
URL : https://www.tecmundo.com.br/seguranca/153157-hackers-invadem-hospital-dizem-bolsonaro-nao-teste-covid-19.htm.

[62] O Globo. *Hackers acessam sistema do Exército e vazam supostos exames antigos de Bolsonaro*. 14 mai 2020.
URL : https://oglobo.globo.com/epoca/brasil/hackers-acessam-sistema-do-exercito-vazam-supostos-exames-antigos-de-bolsonaro-24427224.

[63] NUMERAMA. *Comment l'agence européenne du médicament a-t-elle été piratée ?* 8 mars 2021.
URL : https://cyberguerre.numerama.com/10887-comment-lagence-europeenne-du-medicament-a-t-elle-ete-piratee.html.

[64] DE VOLKSKRANT. *Russian and Chinese hackers gained access to EMA*. 6 mars 2021.
URL : https://www.volkskrant.nl/nieuws-achtergrond/russian-and-chinese-hackers-gained-access-to-ema~bdc61ba59/.

[65] FRANCE INFO. *Covid-19 : l'Agence européenne des médicaments se réunit le 21 décembre sur le vaccin Pfizer-BioNTech*. 15 décembre 2020.
URL : https://www.francetvinfo.fr/sante/maladie/coronavirus/vaccin/vaccin-contre-le-covid-19-l-agence-europeenne-des-medicaments-se-reunit-le-21-decembre-sur-le-vaccin-pfizer-biontech_4220697.html.

[66] CANAL TELEGRAM D'INFINITE INSIGHT. *Revendication d'une Fuite de Données Sur Des Médecins Aux Etats-Unis Par Infinite Insight*. 16 octobre 2023.
URL : https%5B:%5D//t%5B.%5Dme/s/fakesec666/2462.

[67] CISA. *Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities | CISA*. 17 novembre 2021.
URL : https://www.cisa.gov/uscert/ncas/alerts/aa21-321a.

[68] FEDERAL BUREAU OF INVESTIGATION. *Director's Remarks to the Boston Conference on Cyber Security 2022*. 1er juin 2022.
URL : https://www.fbi.gov/news/speeches/directors-remarks-to-boston-conference-on-cyber-security-2022.

[69] U.S. DEPARTMENT OF THE TREASURY. *Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity*. 14 septembre 2022.
URL : https://home.treasury.gov/news/press-releases/jy0948.

[70] ANSSI. *Attaques par rançongiciels, tous concernés*. 4 septembre 2020.
URL : https://cyber.gouv.fr/guide-rancongiciels.

[71] AGENCE DU NUMÉRIQUE EN SANTÉ et CERT SANTÉ. *Observatoire des signalements, d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social*. 21 mai 2024.
URL : https://cyberveille.esante.gouv.fr/sites/default/files/media/documents/observatoire-incidents-cybersecurite-sante-2023.pdf.

[72] ANSSI. *Cartographie du système d'information*. 21 novembre 2018.
URL : https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation.

[73] ANSSI. *La méthode EBIOS Risk Manager*. 18 juillet 2022.
URL : https://cyber.gouv.fr/ebios-rm.

[74] ANSSI. *Externalisation et sécurité des systèmes d'information : un guide pour maitriser les risques*. 3 décembre 2010.
URL : https://cyber.gouv.fr/guide-externalisation.

[75] CLUB RSSI SANTÉ. *Clausier sécurité 2024*. 1er mai 2024.
URL : https://telechargement.rssi-sante.fr/club_rssi_sante_clausier_web_20240627_2024-07-09_08-54-9_374.pdf.

[76] ANSSI. *Recommandations relatives à l'interconnexion d'un système d'information à Internet*. 19 juin 2020.
URL : https://cyber.gouv.fr/guide-interconnexion-si-internet.

[77] ANSSI. *Recommandations relatives à l'administration sécurisée des systèmes d'information*. 11 mai 2021.
URL : https://cyber.gouv.fr/guide-admin-si.

[78] ANSSI. *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory*. 18 octobre 2023.
URL : https://cyber.gouv.fr/guide-admin-si-ad.

[79] ANSSI. *Recommandations Relatives à l'authentification Multifacteur et Aux Mots de Passe*. 8 octobre 2021.
URL : https://cyber.gouv.fr/guide-authentification.

[80] CERT SANTÉ. *Du bon usage d'un EDR*. 22 juin 2023.
URL : https://cyberveille.esante.gouv.fr/du-bon-usage-dun-edr.

[81] ANSSI. *Recommandations de sécurité pour l'architecture d'un système de journalisation*. 28 janvier 2022.
URL : https://cyber.gouv.fr/guide-journalisation.

[82] ANSSI. *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory*. 28 janvier 2022.
URL : https://cyber.gouv.fr/guide-journalisation-windows.

[83] AGENCE DU NUMÉRIQUE EN SANTÉ. *Cybersécurité accélération et Résilience des Etablissements (CaRE) - Gouvernance et Résilience*. 1er janvier 2024.
URL : https://esante.gouv.fr/strategie-nationale/cybersecurite.

[84] ANSSI. *Sauvegarde des systèmes d'information*. 25 octobre 2023.
URL : https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation.

[85] ANSSI. *Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique*. 6 décembre 2021.
URL : https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique.

[86] ANSSI. *Organiser un exercice de gestion de crise cyber*. 14 octobre 2020.
URL : https://cyber.gouv.fr/publications/organiser-un-exercice-de-gestion-de-crise-cyber.

Version 1.0 – 7 novembre 2024

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
cyber.gouv.fr • cert.ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité