MACSF

GUIDE

Cybersécurité

Prévention et bonnes pratiques

PRÉAMBULE

Le secteur de la santé dans la ligne de mire des cybercriminels

Dans sa chronique « Le secteur de la santé dans la ligne de mire des cybercriminels », Loïc Guézo, spécialiste de la cyber-sécurité, rappelle que les donnés médicales sont un bien précieux.

Données médicales : bien précieux

« Les avancées en matière de technologies, et en particulier l'avènement de l'IoT*, ont propulsé **le secteur de la santé à l'ère du numérique**, l'exposant par la même occasion à des menaces plus nombreuses et plus sophistiquées. »

« Les organismes de santé font désormais l'objet d'attaques puissantes à travers le monde. Les données qui y sont stockées et traitées chaque jour sont devenues un bien précieux pour la cybercriminalité souterraine. »

« Les établissements de santé doivent être conscients que les Dossiers Médicaux Electroniques (DME) sont très prisés car synonymes de profit accru pour les cybercriminels, comparé à la simple revente de données personnelles. Ils contiennent en effet une précieuse combinaison de données personnelles, médicales, financières et d'informations liées aux assurances. Or, **ces éléments ont une durée de vie considérable**, contrairement à la nature périssable des données de cartes bancaires. »

➔ **L'enjeu est important, le risque présent, et toujours plus important avec l'avancée de la technologie.**

➔ **La réglementation ne laisse plus de place à l'improvisation, il est temps de prendre les devant !**

*L'Internet des objets, ou IdO (en anglais Internet of Things, ou IoT) est l'interconnexion entre Internet et des objets, des lieux et des environnements physiques

SOMMAIRE

1.
Mieux comprendre les cyber-risques

A. Définitions et quelques chiffres ?

C'EST QUOI UN CYBER-RISQUE ?

Tout risque de perte financière, d'interruption d'activité ou d'atteinte à l'image ou à la réputation visant le système d'information, ainsi qu'aux données stockées ou transférées.

C'EST QUOI UNE CYBERATTAQUE ?

Il s'agit de tout acte de malveillance (divulgation de données confidentielles, accès non autorisés, altération de données, destruction de bases de données...) ayant pour objectif de porter atteinte à un dispositif informatique et de compromettre sa disponibilité, son intégrité ou sa confidentialité.

CHIFFRES CLÉS DE LA CYBERSÉCURITÉ (FRANCE – 2024/2025)

100 Mds €
Coût estimé de la cybercriminalité pour les entreprises françaises en 2024
- (Statista, 2024) -

(Baromètre CESIN, 2025)

46 %
des incidents sont dus à une **erreur humaine**
- (Hiscox, 2024) -

67 %
des entreprises françaises ont subi au moins **1 cyberattaque** en 2024 (53% en 2023)
- (Hiscox, 2024) -

144
rançongiciels traités par l'**ANSSI** en 2024
- (Panorama ANSSI, 2024) -

Secteur de la santé : le plus coûteux en cas de violation de données.

6,83 M€
coût moyen d'une violation → **4,08 M€**
tous secteurs (IBM, 2025)

279 jours
pour détecter et contenir une attaque → **241 jours**
ailleurs (IBM, 2025)

B. Les Cyberattaques les plus courantes dans le secteur de la santé

LES CYBER-ATTAQUES LES PLUS COURANTES DANS LES ENTREPRISES

Types de cyber-attaque les plus constatés par les entreprises françaises en 2018*.

* Plusieurs réponses possibles. En moyenne : 5 types d'attaques parmi ceux ayant subi au moins une attaque. Seules les 10 attaques les plus fréquentes ont été sélectionnées.

Source : **statista**

Le phishing

Le principe de ce type d'attaque repose sur l'envoi d'un email frauduleux contenant une pièce jointe et/ou un lien vers une page malveillante. Ces emails peuvent parvenir parfois d'un expéditeur connu de la victime et dont la boîte mail a été piratée.

Le quishing

Apparition du quishing (QR code piégé) redirigeant vers des portails d'assurance ou de remboursement falsifiés.

En cliquant sur le lien, la victime est redirigée vers une page malveillante qui généralement se présente sous la forme d'une page de connexion, l'invitant à saisir ses identifiants (login et mot de passe). Ce type d'attaques s'appuie principalement sur **les mails comme vecteur principal** de propagation.

➔ **L'objectif principal de ce type d'attaque est de collecter des informations personnelles : mot de passe, numéro de CB...**

L'email reste le premier vecteur de propagation des attaques.

> Selon le rapport Cisco Cyber sécurité 2019

Ransomware

Le Ransomware est un type de malware (logiciel malveillant) qui une fois exécuté va chiffrer les fichiers et les données de la victime. Les données/fichiers ne sont donc plus accessibles, et dans certains cas, les moyens informatiques sont totalement indisponibles.

Le cyber attaquant exige le paiement d'une rançon contre la remise de la clé de déchiffrement permettant de débloquer les moyens informatiques de la victime.

➔ **Ce type d'attaques peut se présenter sous plusieurs formes :**

- **une pièce jointe** dans un mail,
- **un lien** dans le corps d'un mail,
- l'installation d'**un logiciel** infecté,
- **une clé USB** infecté.

L'Agence nationale de la sécurité des systèmes d'information (Anssi) a traité 18 incidents liés à des Ransomware dans le secteur de la santé en 2019.

> Selon un rapport du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) publié le 29 janvier 2020

L'attaque par déni de service distribué

L'Attaque par Déni de Service Distribué (DDOS) consiste à attaquer un système d'information en l'inondant de requêtes lancées à partir de plusieurs machines. L'objectif de cette attaque est de rendre un ou plusieurs services indisponibles et inaccessibles et ainsi d'empêcher des utilisateurs légitimes de l'utiliser.

2.
Les risques

A. Que font les cybers attaquants avec ces données ?

Les Cybers attaquants peuvent réutiliser les données personnelles collectées à plusieurs fins comme par exemple :

- l'organisation **d'autres attaques** plus ciblées de manière massive
- **la monétisation des données personnelles** sur le « Dark Web », chaque type de données personnelles ayant un prix
- **la fabrication de faux papiers administratifs** (passeport, certificat de naissance,...)
- **la mise en vente de fausses ordonnances**
- **la falsification de données financières** et de coordonnées bancaires
- **le détournement des numéros de Sécurité sociale** et bancaires des patients
- **le harcèlement pour soutirer de l'argent** à la victime

Et toutes sortes d'activités criminelles.

ATTENTION

Les motivations des cybers attaquants restent principalement **des motivations financières**.
Le secteur de la santé est **une source de données personnelles et médicales**.

B. Les risques spécifiques au secteur de la santé

Piratage - Vol de données

- Vol des dossiers numérisés avec antécédents médicaux, des résultats d'analyses et traitements en cours.
- Détournement des numéros de Sécurité sociale et bancaires des patients.
- Interruption d'accès aux bases de données.
- Destruction partielle ou totale des informations contenues dans les bases de données.

Paralysie de l'activité

- Le piratage a pour but de ralentir ou stopper l'activité des établissements de santé jusqu'au paiement de la rançon. Les cyber-extorsions représentent un gain financier important.
- Le domaine de la santé est particulièrement visé par les hackeurs, car la sécurité informatique demeure plus faible que dans les autres secteurs d'activités.
- Les équipements médicaux (IR%, machine à rayon X, scanners et autres équipements de diagnostic) sont de plus en plus connectés, sans mise à jour systématique, ce qui représente une faille de sécurité facilement exploitable par les hackeurs.

Nouvelles menaces spécifiques au secteur

MFA Bombing : submersion d'un utilisateur par des demandes d'authentification multifacteur pour le pousser à valider par fatigue.

Infostealers : malwares spécialisés dans le vol d'identifiants (VPN, messageries médicales, dossiers patients).

Supply Chain Attacks : compromission d'un prestataire (ex. hébergeurs certifiés HDS, éditeurs de logiciels santé) impactant de nombreux hôpitaux.

Shadow AI & Deepfakes : utilisation non contrôlée d'outils IA générative pour traiter des données sensibles, ou usurpation d'identité vocale/visuelle d'un médecin pour piéger un service administratif.

EXEMPLES

Viamedis & Almerys (France, 2025) : fuite touchant 33 millions de personnes, incluant données administratives et contractuelles.

Hôpital de Cannes (2023, LockBit) : SI paralysé, services critiques indisponibles.

CHU de Brest (2024) : attaque par ransomware ayant perturbé les soins.

C. Les conséquences liées aux données légales

➔ **Toute information se rapportant à une personne physique identifiée ou identifiable est une donnée personnelle.**

Le 25 mai 2018 est entré en vigueur le Règlement Général sur la Protection des Données (RGPD) qui harmonise au niveau européen la réglementation sur la protection des données personnelles.

Le RGPD prévoit que tous les organismes (associations, entreprises…) sont responsables quelque soit les secteurs d'activité.

Le 18 octobre 2024 est entrée en vigueur en France la directive européenne **NIS2**, qui renforce le cadre de cybersécurité.

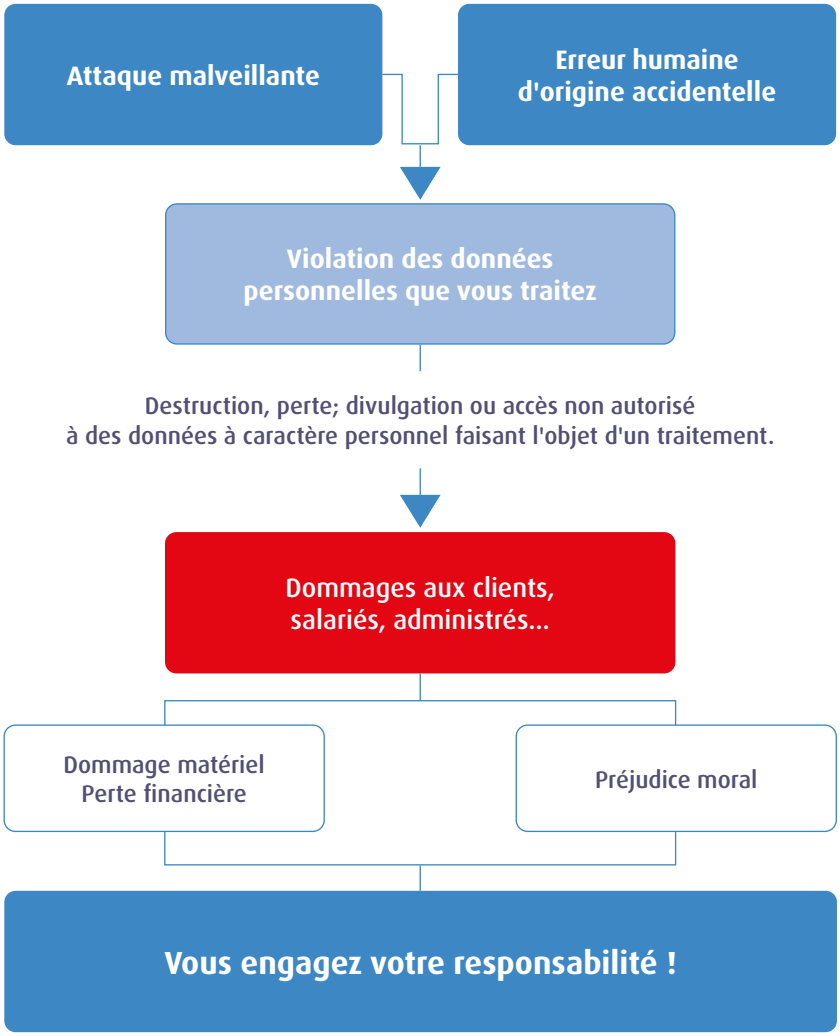
Elle classe notamment les établissements de santé parmi les entités essentielles et leur impose des obligations accrues, dont la notification des incidents de sécurité dans un délai de 24 heures.

En 2025 a été adopté l'**AI Act**, le règlement européen encadrant l'usage de l'intelligence artificielle.

Il fixe des règles strictes pour les systèmes considérés à haut risque, en particulier ceux qui traitent des données médicales sensibles, afin de garantir la sécurité, la transparence et la protection des patients.

Pour faire face à la divulgation des données patients, à l'interruption de l'activité, à une atteinte à la réputation, demande de rançon, une sanction administrative... **l'assurance Cyber Risques est la solution.**

> En savoir plus sur l'assurance Cyber Risques MACSF.



Contacter un client pour lui indiquer que vous vous êtes fait voler ses données personnelles coûte, selon les estimations, entre 50 et 150 € par client.

Source : « 2018 Cost of a data breach », IBM-Ponemon.

3.
La prévention des cyber-risques

A. Comment se protéger ?

	Les bons réflexes !
Mails et réseaux sociaux	➔ **Ne pas ouvrir les pièces jointes et ne pas suivre les liens contenus dans les mails à contenu** suspect (demande de virement, demande urgente…) ou provenant de destinataires inconnus ➔ **Ne jamais répondre au mail d'un expéditeur suspect** et le placer directement dans la corbeille ➔ **Ne jamais cliquer sur les liens raccourcis** sur les réseaux sociaux ➔ **Ne jamais répondre par mail aux demandes d'informations personnelles et confidentielles** ➔ **Ne jamais transmettre de données personnelles ou médicales sensibles par email.**
Sauvegardes	➔ **Effectuer régulièrement des sauvegardes** de vos données en utilisant **des supports externes** dédiés à cet usage ➔ Placer tous les supports de stockage amovibles **dans un coffre-fort ou dans une armoire à clé**
Dispositifs techniques	➔ **Installer et mettre à jour régulièrement un antivirus** supporté par son éditeur, non téléchargé gratuitement sur internet ➔ **Installer un pare-feu** sur votre poste de travail et le maintenir à jour ➔ **Chiffrer les données sensibles** (dossiers médicaux…) en utilisant un logiciel de chiffrement adapté ➔ **Mettre à jour le système d'exploitation** et les applications ➔ **Recourir à des solutions EDR/XDR pour détecter et neutraliser** rapidement **les ransomwares et infostealers**. ➔ **Mettre en place une segmentation réseau afin d'isoler les équipements médicaux connectés** (IoMT).
Accès et mot de passe	➔ **Renouveler les mots de passe** régulièrement (tous les 90 jours) ➔ Choisir **un mot de passe non lié à votre identité** (nom, prénom, date de naissance…) ➔ Utiliser des mots de passe robustes : **au moins 12 caractères** (majuscules, minuscules, chiffres, symboles). ➔ **Refuser systématiquement la mémorisation** de votre mot de passe sur les sites ➔ **Sécuriser l'accès à votre wifi** via l'utilisation d'un mot de passe complexe ➔ Utiliser **l'authentification à facteurs multiples** ➔ Avoir **des mots de passe différents** pour chaque application/compte ➔ Utiliser **un coffre-fort de mots de passe**, s'assurer que le logiciel est sécurisé CSPN ➔ **Gérer les droits d'accès et limiter les accès** aux fichiers et aux documents à caractère confidentiel et au contenu sensible

4.
Lexique

Lexique

Darkweb
Pages Internet accessibles uniquement via des navigateurs spéciaux. Elles sont notamment le lieu d'activités illégales (vente de données, de drogues...).

Déni de service
(DoS)
Action (malveillante ou accidentelle) qui a pour résultat de bloquer ou de ralentir un système d'information. Si elle est lancée à partir de plusieurs machines, on parle alors de « Déni de service distribué » (DDoS).

Hameçonnage
(ou « phishing » en anglais)
Technique qui consiste, pour les pirates informatiques, à envoyer un mail aux couleurs d'un partenaire ou d'un prestataire de confiance, dans le but de dérober des informations.

Harponnage
(ou « spear-phishing » en anglais)
Une déclinaison de l'hameçonnage, qui s'appuie sur une connaissance de la cible et une personnalisation du message.

Homme du milieu
(ou « man in the middle » en anglais)
Technique à travers laquelle un pirate informatique intercepte les données échangées entre deux parties, à leur insu.

Ingénierie sociale
(ou « social engineering » en anglais)
Manipulation psychologique exercée dans le but d'obtenir la confiance de la victime et de lui soutirer des informations, de l'argent...

Logiciel malveillant
(ou « malware » en anglais)
Programme informatique destiné à nuire à un système informatique. Il peut prendre la forme par exemple d'un rançongiciel ou encore d'un botnet.

Pare-feu
(ou « firewall » en anglais)
Outil permettant de protéger les ordinateurs connectés à un réseau. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant).

Rançongiciel
(ou « ransomware » en anglais)
Logiciel malveillant qui crypte les données de ses cibles, avant de demander le paiement d'une rançon pour le déblocage des informations retenues en otage.

Réseau de machines zombies
(ou « botnet » en anglais)
Ensemble de machines infectées par un logiciel malveillant et utilisées par les pirates informatiques, le plus souvent dans le cadre d'attaques DoS.

Shadow IT
Logiciels installés sur des ordinateurs professionnels sans l'autorisation préalable de la DSI.

Test d'intrusion
(ou « pentest » en anglais, pour « penetration test »)
Attaque menée contre son propre réseau, afin d'en détecter les failles de sécurité.

Ver
Logiciel malveillant qui se caractérise par sa capacité à se propager et s'exécuter en toute autonomie, sans programme hôte (tel qu'un fichier exécutable).

Virus
Logiciel malveillant qui se diffuse à partir de programmes hôtes (tel qu'un fichier exécutable).

MACSF

La MACSF accompagne les professionnels de santé
dans leur exercice au quotidien :

Nous contacter

Ensemble, prenons soin de demain

25_695 - 10/2025.