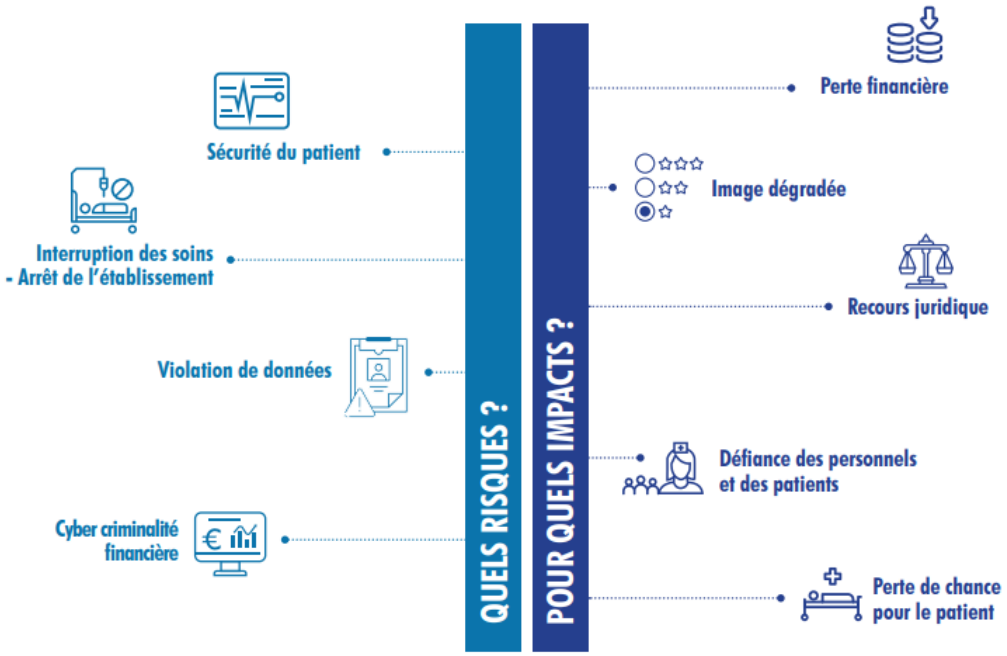
ALERTE CYBERSECURITE à destination des praticiens

Les systèmes informatiques des centres de soins sont une cible privilégiée des cyberattaques, du fait de la généralisation d'usages numériques mal maitrisés et de la spécialisation et de la professionnalisation de l'écosystème cybercriminel. L'année 2021 a été marquée par de nombreux incidents majeurs : attaques par rançongiciel (CH Dax, Villefranche-sur-Saône ou Arles) ou exfiltration massive de données (APHP, CNAM). Au total, l'Agence du Numérique en Santé a déploré **en 2021, 730 incidents** (contre 369 en 2020). Ces cyberattaques impactent le domaine de la santé en perturbant le quotidien des professionnels et/ou en mettant en péril la prise en charge des patients.



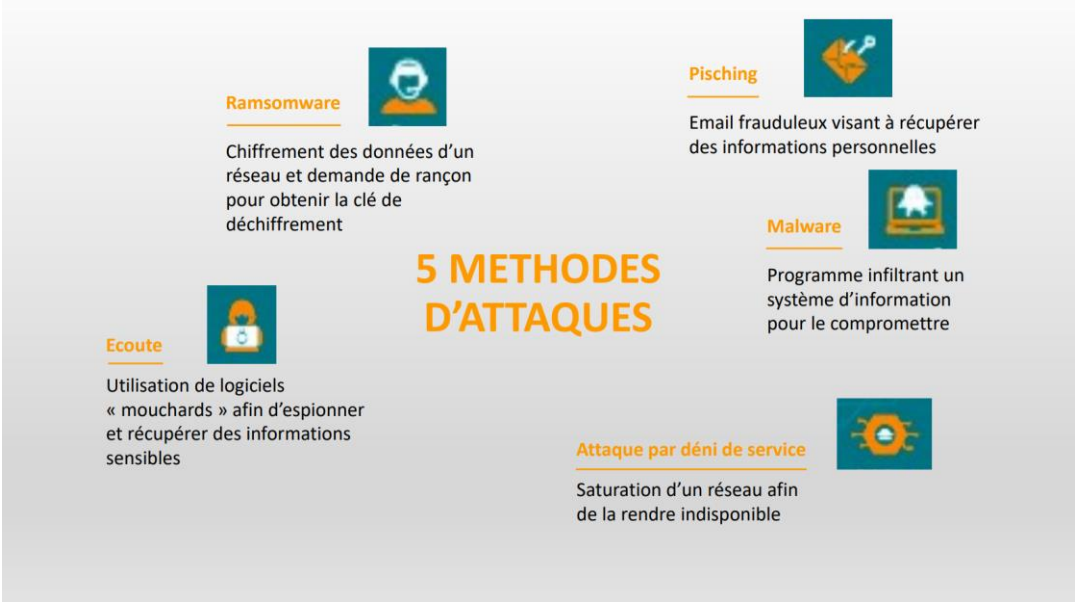
UN EQUILIBRE DIFFICILE A TROUVER

La sécurité informatique cherche à résoudre une dualité d'usage : assurer la sécurité d'un système informatique, qui dans l'absolu reviendrait à avoir un système totalement fermé, et permettre aux utilisateurs légitimes de travailler sans entraver leur usage opérationnel. La sécurité informatique navigue donc en permanence entre ces 2 pôles : sécuriser et permettre un usage sans entrave.

QUEL TYPE D'ATTAQUE ?

60% des incidents déclarés ont une origine malveillante (+17% par rapport à 2019)

Le piratage exploite les faiblesses psychologiques, sociales et plus largement organisationnelles, des individus ou organisations pour obtenir quelque chose frauduleusement. Cette pratique de manipulation utilise principalement les « failles humaines » d'un système d'information comme « effet de levier », pour briser ses barrières de sécurité.
L'hameçonnage (*phishing*) en est un exemple. Il s'agit d'une technique frauduleuse destinée à leurrer un utilisateur pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) en se faisant passer pour un tiers de confiance.
Mais la principale forme d'attaque se fait avec un **maliciel (ou logiciel malveillant)** qui permet d'infiltrer l'ordinateur et/ou d'endommager le système. Il peut être de plusieurs types : logiciel espion, virus, ransomware, cheval de troie, rookit…
Les intentions des acteurs malveillants restent le gain financier, la donnée de santé étant précieuse et en devient donc monnayable. D'autres objectifs peuvent intervenir (espionnage, déstabilisation du système de soin).



PREVENIR ….

Si aucun système informatique est infaillible, la majorité des attaques informatiques peuvent être prévenue par le biais d'une **formation des utilisateurs** du système de soin (respect des règles de sécurité des mots de passe par exemple). Accessible à tous, l'agence nationale de la sécurité des systèmes d'information propose une formation (MOOC) concernant les risques liés à la cybersécurité.
Outre la nécessité de formation de tous les utilisateurs du réseau, un **plan d'action en cas de dysfonctionnement** des systèmes informatiques dédié doit être travaillé au sein de chaque structure de soin. Ce plan d'action doit être connu de tous, et disponible au format papier pour tous les services de soins.

… POUR EVITER DE GUERIR

Au moment d'une cyberattaque, les moyens de lutte sont limités pour le praticien. De manière pragmatique, une **déconnexion mécanique du réseau** (arrêt du Wifi, ou débranchement de la prise réseau) sera la priorité pour éviter la propagation de l'attaque ou la fuite de données. La machine devra être laissée sous tension pour permettre un diagnostic exhaustif. Le service support informatique devra être rapidement contacté pour investiguer et corriger les éventuels dommages laissés par l'attaque.

Fiche reflexe ANS:
https://esante.gouv.fr/sites/default/files/media_entity/documents/PGSSI_S-Guide_Orga-Memento_PS_Exercice_Liberal-Annexe_2-Fiche_reflexe_incident-V2.0.pdf

En cas de dysfonctionnement du matériel informatique à l'échelle de la structure hospitalière, le plan d'action prévu en amont par chaque établissement devra être rapidement mis en place, ainsi que l'instauration d'une cellule de crise dédiée à la problématique.

SIGNALEMENT

Finalement, **l'incident devra être déclaré** sur cybermalveillance.gouv.fr, et suivant le type d'attaque, à la CNIL en cas de fuite de données patients.

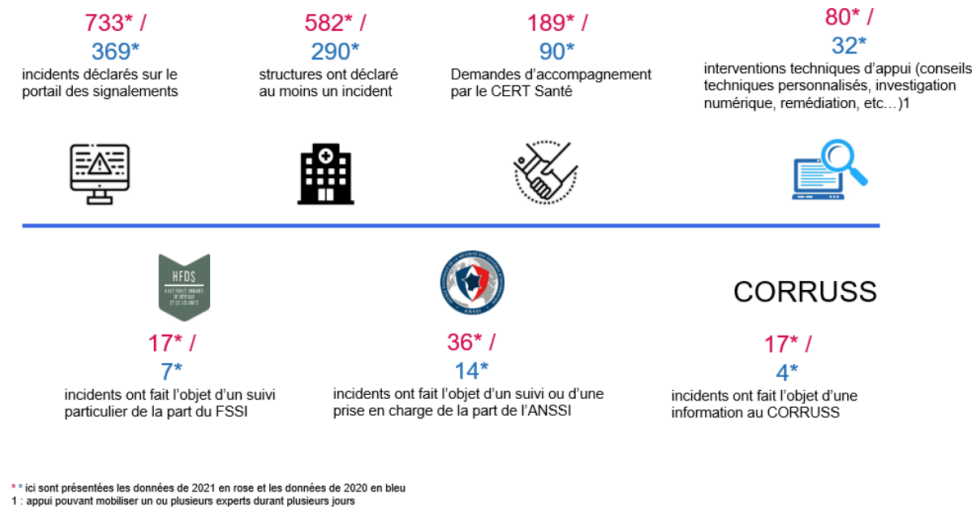


Figure 1 – Chiffres clés des signalements déclarés en 2020 et 2021

MOOC SECNUMACADEMIE : Formation sur la sécurité du numérique [https://www.ssi.gouv.fr/administration/formations/secnumacademie/]

Guide d'hygiène informatique de l'ANSII [https://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/]

Guide de bonne pratique en sécurité informatique de l'ANS [https://esante.gouv.fr/actualites/lans-publie-un-memento-de-securite-informatique-pour-les-professionnels-de-sante-en-exercice-liberal]

Rapport 2021 de l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé.
[https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2021_vf.pdf