CYBERSÉCURITÉ :
QUELQUES RÈGLES CLÉS À RESPECTER

ORGANISATION

- GOUVERNANCE PAR LE MANAGEMENT DES RISQUES
- CARTOGRAPHIE DES RISQUES QUI PREND EN COMPTE LE RISQUE CYBER
- UN (E) RESPONSABLE EN CHARGE DE LA SÉCURITÉ DU NUMÉRIQUE (RSSI)
- UN (E) DÉLÉGUÉ (E) À LA PROTECTION DES DONNÉES PERSONNELLES
- PRISE EN COMPTE DE LA SSI DANS LES BUDGETS SI (≈10%)

SÉCURISATION

- PLAN D'ACTION CYBER MIS À JOUR EN CONTINU
- RÉALISER RÉGULIÈREMENT DES AUDITS DE SÉCURITÉ
- NÉCESSITÉ DE MAINTENIR DES SAUVEGARDES HORS RÉSEAU (CE QUI DIMINUE LARGEMENT LES IMPACTS D'UNE ATTAQUE PAR RANÇONGICIEL)

SENSIBILISATION

- FORMER AUX ENJEUX DE LA CYBERSÉCURITÉ ET AUX PRINCIPES D'HYGIÈNE NUMÉRIQUE
- RAPPELER LES RÈGLES D'USAGE EN MATIÈRE D'UTILISATION DE LA MESSAGERIE

GESTION DES INCIDENTS

- DÉFINIR ET FAIRE CONNAITRE LA PROCÉDURE D'ALERTE ET DE RÉACTION EN CAS D'INCIDENT
- RÉALISER DES EXERCICES DE CONTINUITÉ D'ACTIVITÉ EN MODE "NUMÉRIQUE DÉGRADÉ"
- DÉCLARER TOUT INCIDENT SI SUR LE PORTAIL DE SIGNALEMENT DES ÉVÈNEMENTS SANITAIRES

POUR DÉCLARER VOS INCIDENTS :

https://signalement.social-sante.gouv.fr
Allez dans la rubrique "Vous êtes un professionnel de santé"

POUR ACCOMPAGNER LE SECTEUR SANTÉ :

LE CERT SANTE

Le signalement des incidents de sécurité des systèmes d'information des structures de santé est obligatoire depuis le 1er octobre 2017.

LES 3 MISSIONS DU CERT SANTÉ

1. L'APPUI dans le traitement des incidents de Cybersécurité
2. LA VEILLE SUR LA MENACE de Cybersécurité et la sensibilisation de la communauté
3. AUDIT DE CYBERSURVEILLANCE et action de prévention

PORTAIL DE VEILLE, D'ALERTE ET D'ÉCHANGE :
www.cyberveille-sante.gouv.fr

CONTACTER LE CERT SANTÉ :
cyberveille@esante.gouv.fr
+33 (0)9 72 43 91 25
Permanence les jours ouvrés de l'ANS, 9h-18h

CONTACTER HFDS/FSSI :
ssi@sg.social.gouv.fr

CONTACTER L'ANSSI :
cert-fr.cossi@ssi.gouv.fr

l'agencevelte

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

LA SÉCURITÉ NUMÉRIQUE, SOCLE DE LA « TRANSFORMATION DU NUMÉRIQUE EN SANTÉ »

HFDS
MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

TOUS CYBER VIGILANTS

INVESTISSEMENT : 350 millions d'euros issus des 2 milliards d'euros du Ségur de la santé consacrés au numérique seront dédiés à renforcer la sécurité des systèmes d'information de santé impliqués dans les échanges de données du parcours.

RÉPONDRE À LA MENACE DE CYBERSÉCURITÉ PAR :

- UNE PRISE DE CONSCIENCE COLLECTIVE ET INDIVIDUELLE
- UN ACCOMPAGNEMENT ET UN APPUI RENFORCÉ AUX STRUCTURES DE SANTÉ
- UN INVESTISSEMENT DANS LA DURÉE : LE SÉGUR DE LA SANTÉ

Notre stratégie nationale en matière de cybersécurité va accélérer. Car il nous faut aller plus loin, plus vite, être à l'avant-garde. Au total, 1 milliard d'euros seront investis.

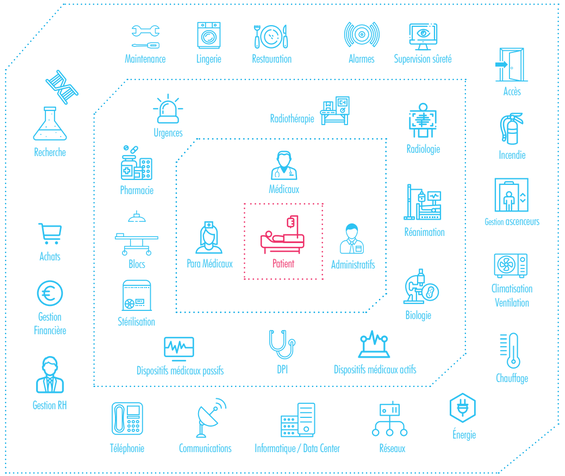
Emmanuel Macron, 18/02/2021

Il est nécessaire pour le ministère de renforcer et d'améliorer sa politique en matière decybersécurité, pour aider les établissements à faire face à des actes de cyber malveillance de plus en plus sophistiqués et d'inciter les acteurs à plus de responsabilité et plus de pédagogie. Alors je vous le demande, soyons TOUS CYBERVIGILANTS !

Olivier Véran, 18/02/2021

COMPRENDRE LES CYBER-RISQUES : UNE NÉCESSITÉ

Aujourd'hui la quasi-totalité des activités du secteur santé reposent sur le numérique et ont des impacts directs ou indirects sur la prise en charge comme l'ont démontré des incidents récents (exemples : impacts de la téléphonie, de la climatisation, de la stérilisation, des ascenseurs, et bien sûr les plateaux techniques et le DPI).
La sécurité numérique doit donc bénéficier d'une approche globale.



QUELLES SONT LES PRINCIPALES VULNÉRABILITÉS D'UNE STRUCTURE DE SANTÉ ?

LOGICIELS/SYSTÈMES NON CORRIGÉS OU OBSOLÈTES

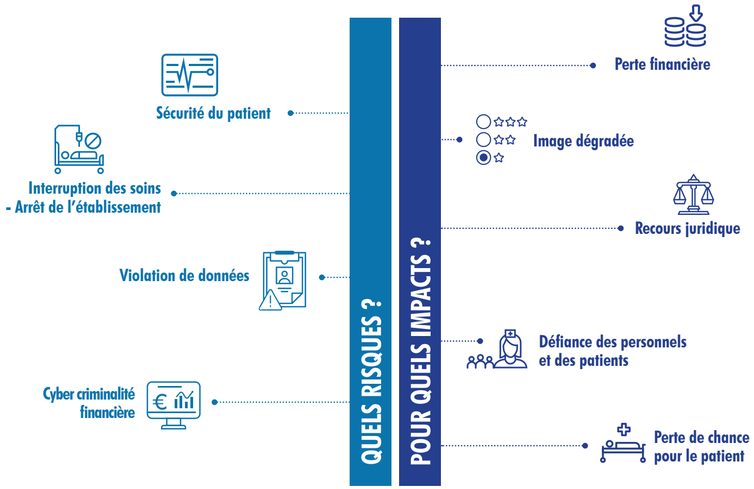
MANQUE DE VISIBILITÉ ET D'INVENTAIRE DES SYSTÈMES NUMÉRIQUES

CONTRÔLES INSUFFISANTS DE LA CYBERSÉCURITÉ DES SYSTÈMES PÉRIPHÉRIQUES

GRANDE VARIÉTÉ DE PROTOCOLES, DE FOURNISSEURS ET DE PÉRIPHÉRIQUES MANQUE D'OPÉRABILITÉ

COMPOSANT CRITIQUE DU SI INSUFFISAMMENT SÉCURISÉ (SAUVEGARDE, ACTIVE DIRECTORY)

COMPLEXITÉ DUE À DES RESPONSABILITÉS DIFFUSES DSI - BIOMÉDICAL - MOYENS GÉNÉRAUX...



QUELQUES CHIFFRES CLÉS

847
INCIDENTS DÉCLARÉS
depuis 2017

Depuis le printemps 2019, une quarantaine d'établissements ont déjà été analysés.

Une croissance de la menace confirmée en 2020 (Observatoire des incidents de sécurité)

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

58% **DES INCIDENTS ONT EU UN IMPACT SUR DES DONNÉES** (disponibilité des données principalement)

42% des incidents sont des maliciels.

35% sont liés à une activité de phishing.

42% sont liés à l'exploitation d'une vulnérabilité sur un accès à distance.

24% des signalements ont donné ensuite lieu à un accompagnement par le CERT Santé.

81% des incidents de sécurité est déclarée par les établissements de santé.

45%
C'est le pourcentage de structures qui ont été contraintes à mettre en place en 2020 un fonctionnement en mode dégradé du système de prise en charge des patients.

ÇA PEUT VOUS ARRIVER :

- Des établissements de santé et du médico-social sont régulièrement victimes d'attaques par rançongiciel. Cela les a contraints à travailler en mode dégradé pendant plusieurs semaines.
- Le chiffrement des données entraine l'arrêt des activités et la perte éventuelle des données.