LES CYBERATTAQUES CONTRE DES CENTRES HOSPITALIERS

On parle de cyberattaque,

si une personne ou un groupe tente d'accéder frauduleusement à un système informatique.

L'OBJECTIF DES PIRATES ?

Perturber le fonctionnement du système pour le rendre inutilisable

Dérober les données sensibles qu'il contient pour les monnayer

Les établissements hospitaliers sont des **cibles privilégiées** pour les pirates du web :

les établissements de santé concentrent de nombreuses données sensibles,

leur sécurité numérique est encore en construction.

Comment se déroule une cyberattaque ?

1

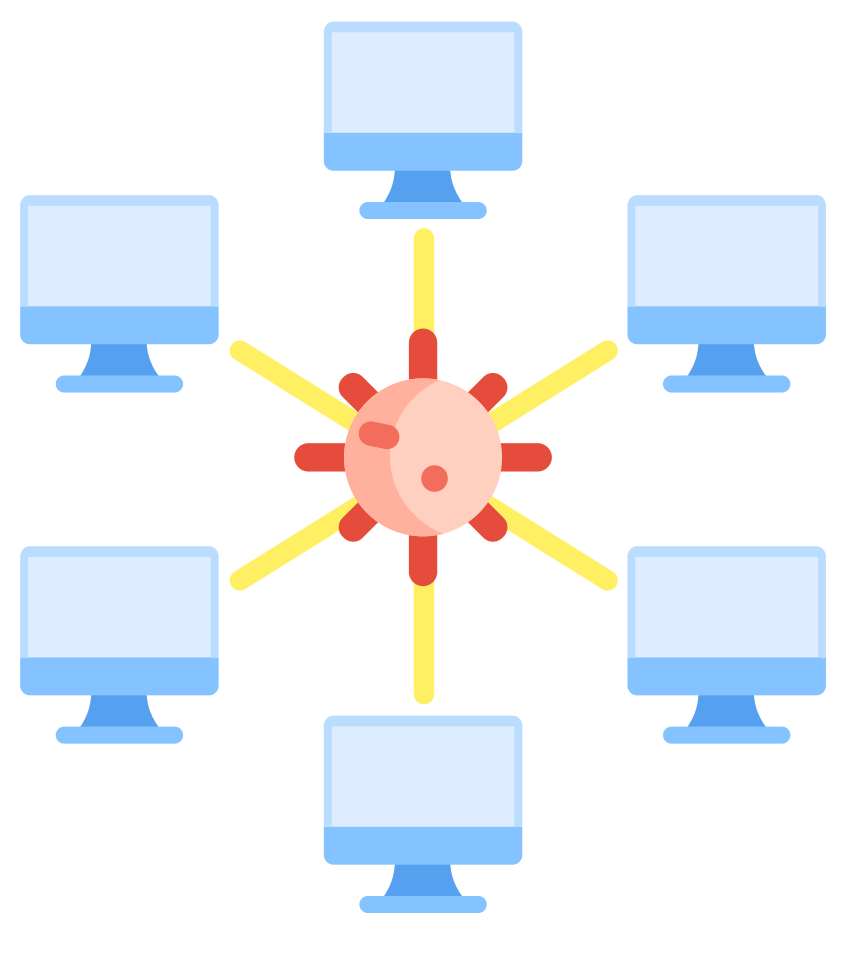
Un fichier virussé est envoyé sur la boîte mail d'un personnel d'établissement de santé.

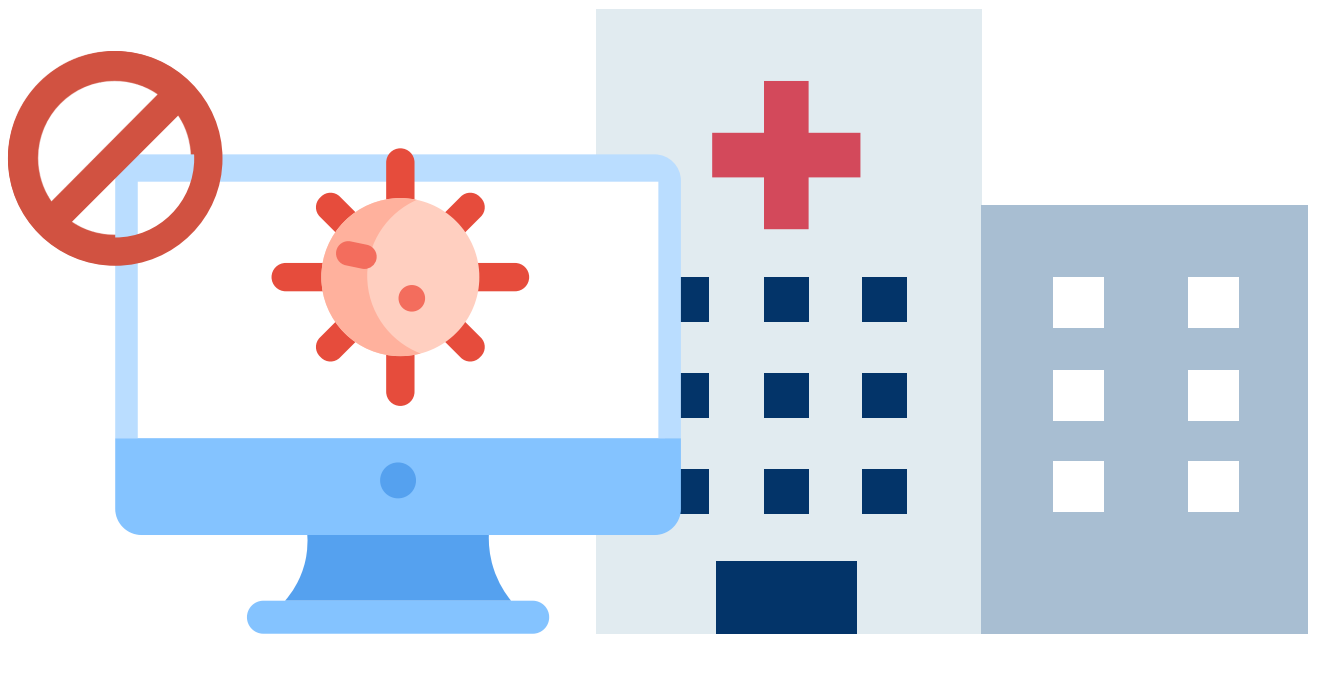
2

Son ouverture active le virus.

3

Le matériel informatique fonctionnant en réseau, le virus se diffuse très rapidement à l'ensemble de l'établissement.





4

L'intégralité du système informatique de l'établissement est paralysée.

LES PIRATES UTILISENT GÉNÉRALEMENT UN RANÇONGICIEL

qui **chiffre les données de l'établissement** et les rend inaccessibles tant qu'une rançon n'a pas été payée.

Ils peuvent aussi **faire fuiter les données volées sur le web** ou **les revendre**.

Problème,

les données traitées par un établissement de santé sont **très sensibles** :

Identité des patients
(nom, prénom, date de naissance, n° de sécurité sociale)

Compte-rendus d'examens médicaux confidentiels

Documents externes personnels
(résultats de laboratoires d'analyse, autorisation d'internement d'office en service psychiatrique…)

Le piratage oblige également l'établissement visé à passer en **mode dégradé :**

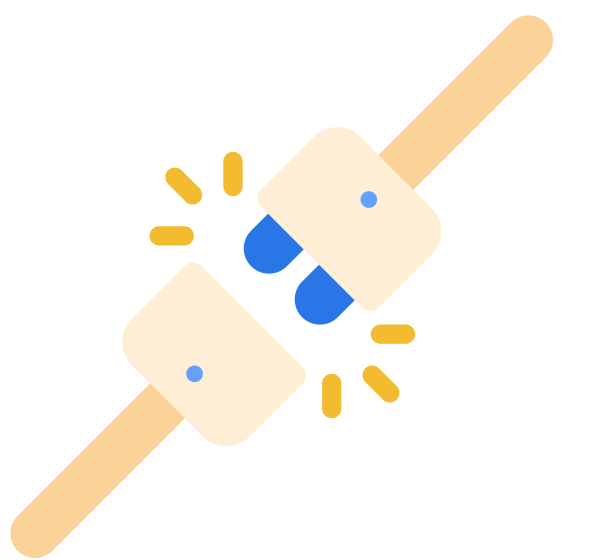
Aucun enregistrement possible
de nouveau patient

Déprogrammation
de certains actes médicaux et opérations

Transfert
de certains patients vers d'autres centres hospitaliers

Aucun établissement n'est à l'abri !

Quels bons réflexes en cas de cyberattaques ?



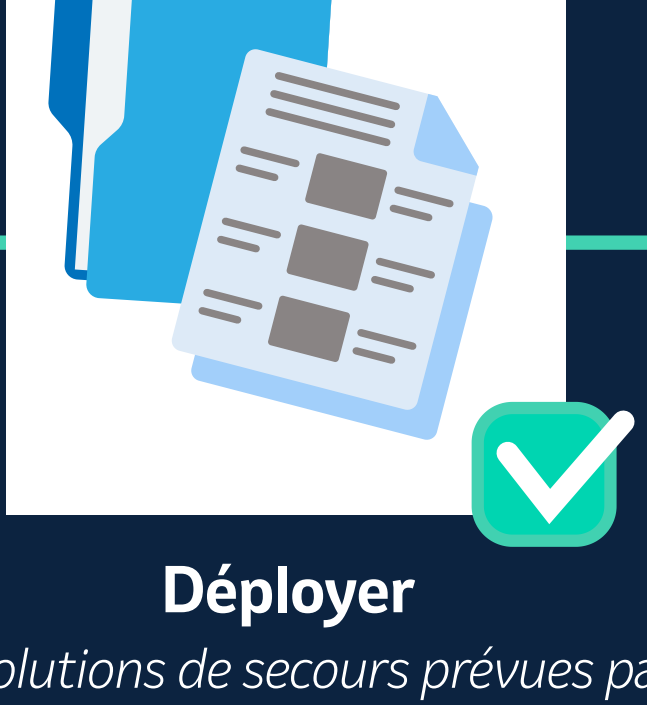
Déconnecter
tous les systèmes du réseau local et d'Internet

Alerter
votre support informatique, le prestataire en charge de la cybersécurité, et l'ARS

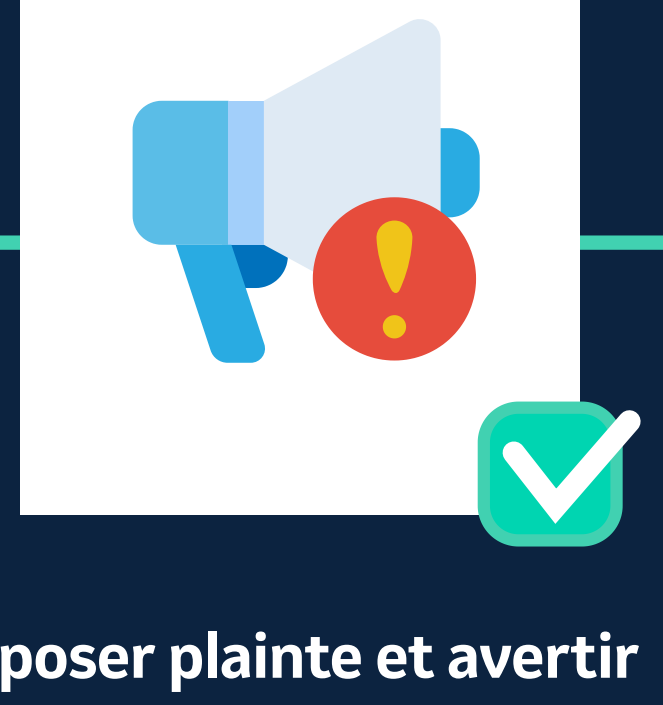
Constituer
une équipe de gestion de crise et documenter les évènements

Ne jamais payer de rançon !

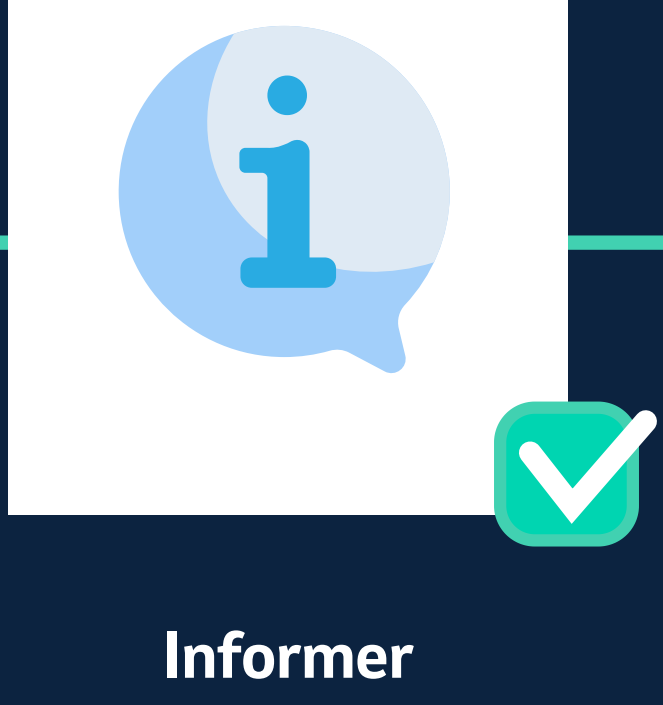
Comment gérer la crise et en sortir ?



Déployer
les solutions de secours prévues par votre Plan de Continuité d'Activité



Déposer plainte et avertir
la CNIL dans les 72h si des données personnelles ont été ciblées



Informer
vos partenaires et les personnes impactées avec le juste niveau de transparence

Identifier
la faille à l'origine de l'attaque et mettre en place les actions correctives nécessaires

Faire une remise en service progressive et contrôlée
une fois la sécurité de votre infrastructure informatique rétablie

MSD

Réalisé par sydo

FR-AAM-00204 Avril 2023