Maison d'accueil Le Bois Hercé

EHPAD Nantais de 80 résidents

Situé en ville avec petit parc, à proximité du tramway

Au sein de l'Association St Joseph comptant 2 EHPAD et 1 accueil de jour

Serveur virtualisé, double sauvegarde

Certains logiciels extérieurs (soins, maintenance) et hébergés sur place (compta, paye, facturation)

Attaque d'un crypto locker
début juillet 2018 – jour 1

- Les fichiers, devenus grisés, changeaient progressivement d'extension. Ceci progressivement à un rythme différent selon les postes de travail.
- Tous les fichiers étaient infectés dans l'espace de moins d'une heure.
- Appel du prestataire informatique qui intervient rapidement
  - Effacement des fichiers et remplacement par une sauvegarde.
    - Possible par la « virtualisation » du serveur (intervention à distance)
-  Défaut de sauvegarde
  - Sauvegarde NAS éteinte (sans doute lors d'un essai de groupe électrogène engendrant une micro coupure)
  - Sauvegarde sur cassettes défectueuse (cassettes pleines et réécriture partielle)
  - 2 jours de traitement
- Données récupérées à fin février !

Attaque d'un crypto-locker
début juillet 2018 – jour 2 et 3

- Le lendemain de la restauration : nouvelle attaque du même virus
  - Nouvelle restauration de la sauvegarde faite la veille
- Le virus est revenu une 3ème fois
  - Le nettoyage et la restauration de la sauvegarde ne suffisent pas

Traitement

- Un serveur virtuel a été créé à la 1ère restauration, tout en gardant l'ancien (garder le contact avec le serveur physique)
  - Décision prise de « détruire » le serveur d'origine. Le virus était caché dans le méandre des milliers de fichiers (aiguille dans une botte de foin)

Impact

- Entre 2 et 4 mois de données perdues
  - Fichiers de travail présents sur le serveur (4 mois)
  - Mémoires d'aide sociale, facturation des résidents
  - Données comptables et salariales
- Préservation des données de soins : logiciel de gestion des soins externalisé

Décisions prises

- Supprimer les failles de sécurité
  - Accès distant au serveur sans connexion VPN
  - Les utilisateurs pouvaient aller sur internet par le serveur
- Prise en compte effective du risque numérique
  - Créer une connexion distante VPN
  - Bloquer l'accès à internet à partir du serveur (modifier la configuration des postes légers)
  - Externaliser tous les logiciels métier (suppression du serveur physique), ne garder que la sauvegarde