LE GUIDE DU GBM

# LA CYBERSÉCURITÉ

Cyber Security

## QU'EST CE QUE C'EST ?

La cybersécurité concerne la **protection des systèmes informatiques**, des appareils et des données sensibles utilisés dans la recherche, le diagnostic et le traitement des patients **contre les intrusions malveillantes** visant à voler, altérer ou détruire des données sensibles (= dossiers médicaux ou résultats de recherche).
Aujourd'hui, avec l'essor des technologies numériques dans le secteur de la santé, le domaine biomédical est une **cible privilégiée** pour les cyberattaques.


## CONSÉQUENCES D'UNE MAUVAISE SÉCURITÉ

- **Dysfonctionnements dangereux**, qui peuvent entrainer un risque pour les patients.
- **Divulgation de données médicales**, entraînant des risques pour la vie privée des patients.
- **Paralysie des services de santé**, entraînant un retard des traitement et une nuisance aux soins.

## ACTEURS

- **Hôpitaux et cliniques** : principales cibles, doivent former leur personnel.
- **Fournisseurs de dispositifs médicaux** : garantir la bonne sécurité contre les attaques.
- **Hackers et cybercriminels** : principaux auteurs des attaques, motivés par des gains financiers, la recherche d'informations et/ou la perturbation.

## COMMENT SÉCURISER DES SYSTÈMES D'INFORMATION ?

**La formation du personnel** : organisation de sessions de travail pour sensibiliser sur le sujet. Certains établissements établissent également des tests sur leur personnel, afin de mener au mieux leur campagne de sensibilisation.
**Promotion des règles de bases** : comme le changement régulier des mots de passe ou l'isolement de mails indésirables, chez les utilisateurs (patients ou personnels) pour limiter les potentielles attaques
**Les mesures de sécurisation** : privilégier des applications de travail (gestion des patients, imagerie médicale...) fonctionnant avec les mêmes versions de système ou des logiciels compatibles entre eux. De plus, il ne faut pas minimiser les infrastructures et les systèmes d'exploitation sur lesquels reposent ces applications, car leur vulnérabilité peut être exploitée par des cybercriminel pour infiltrer les systèmes.
**La stratégie "Zéro Trust"** : il est préférable de restreindre strictement les accès aux différents systèmes, car les attaques peuvent aussi bien venir de l'intérieur comme de l'extérieur.