TÉMOIGNAGE

CYBER-ATTAQUE AU SEIN D'UN SERVICE DE RADIOLOGIE D'UNE CLINIQUE DE NOUVELLE AQUITAINE

Nous savions que nous serions attaqués... nous ne savions simplement pas quand ?

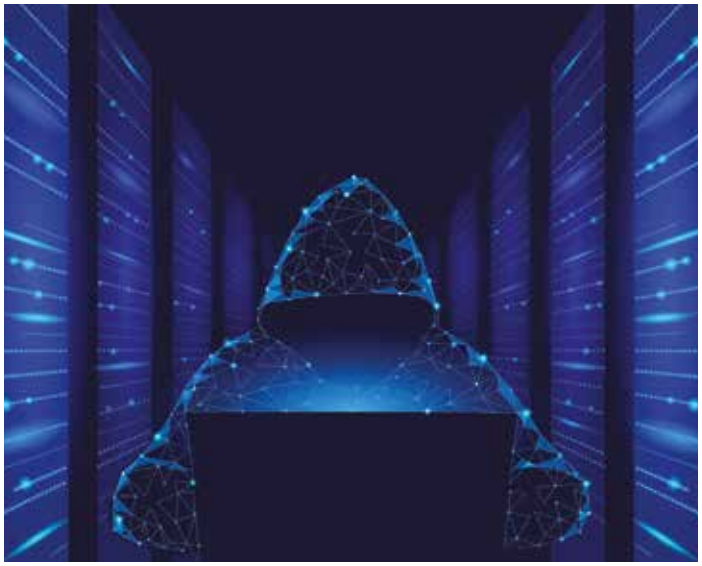
Les médecins sont responsables et garants des données de Santé qu'ils collectent et conservent sur leurs serveurs informatiques, selon le Règlement Général sur la Protection des Données (RGPD) de 2018.
Les données de santé sont qualifiées par la CNIL de « données sensibles ». Elles ont actuellement une importante valeur marchande (10 fois plus importante que les données d'une carte bleue).

Nécessité de sensibiliser la profession au RGPD, rôle du délégué à la protection des données (DPO) dans les groupes.

Des « pirates » informatiques se spécialisent dans la détection et l'utilisation de failles dans les réseaux.

Pensez à la mise à jour de tous les logiciels - optimisation du paramétrage du pare-feu de la box internet - utilisation de mots de passe complexes - se faire aider par son prestataire informatique.

Durant l'été, des hackers ont utilisé une faille de sécurité d'un logiciel métier au sein de notre établissement pour pénétrer sur le réseau de la clinique. L'attaque a eu lieu, comme souvent, dans la seconde partie de la nuit en semaine. La première cible a été les « serveurs directory » où sont colligés les identifiants et les mots de passe des administrateurs réseau. Cette activité inhabituelle sur le réseau a été détectée comme suspecte par les moyens mis en œuvre par le Directeur des Services Informatiques (DSI) de l'établissement. Les serveurs ont immédiatement été coupés et l'établissement a été isolé du web...
Puis, un virus « dormant » déposé lors de l'attaque initiale s'est activé le week-end sur notre propre réseau du service d'imagerie, qui comporte des passerelles avec le réseau de l'établissement. Il a immédiatement été détecté par les moyens de surveillance mis en œuvre en moins de 24 heures après la première attaque. Ceci nous a obligé à nous isoler de l'établissement et à nous couper de l'internet.



Attention aux effets rebond d'une attaque, avec propagation aux autres utilisateurs.

La cyber-attaque a ainsi été bloquée. Quelles auraient pu être les conséquences ?

- La responsabilité du médecin est engagée et il doit se plier à des formalités administratives : déclaration en ligne à la CNIL, dépôt de plainte aux services de police.
- L'obligation de restructurer le système informatique et d'accroitre les mesures de sécurité. L'analyse de l'attaque a paralysé l'établissement durant une bonne semaine. La restructuration a obligé à un fonctionnement dégradé durant 4 mois avant un retour à la normale. Tout cela a ainsi un retentissement financier.

En pratique :

- Altération de l'image de marque si l'attaque avait été réussie, avec divulgation dans la presse.
- Regarder si votre assurance inclut les cyber-risques et vérifier les clauses de prise en charge.
- Dans l'hypothèse d'une utilisation multi sites de vos données, renseignez vous auprès de votre partenaire informatique pour installer un VPN* (communication sécurisée).

Notre réactivité et nos moyens de défense ont évité la capture ou la perte de données sensibles, ainsi qu'une éventuelle rançon si les données avaient été cryptées - la cyber-attaque n'est pas la guerre de demain... c'est la guerre d'aujourd'hui.

Protégez vos données dès maintenant, en adoptant les bonnes mesures.

Eteignez vos PC la nuit et le WE si vous n'en avez pas l'utilité - renforcez les moyens de surveillance informatique automatique dans les grosses structures.

* Virtual Private Network