A quoi faut-il penser en cas de cyber attaque / panne informatique

Que faut – il prévoir ?
Comment anticiper ?

Journée des membres
3/12/2022

Administrateurs ASTER

Avant toute chose :

Une cyber attaque ne se prévoit pas, il faut donc anticiper et prévenir d'éventuels problèmes

1) **Prévoir un fonctionnement en procédure dégradée :**

- mettre en place un bon système de communication : direction - bloc opératoire - stérilisation – pharmacie;

- définir la prise de décision du "GO" suivant un arbre décisionnel claire et validée par tous;

- créer les procédures en mode dégradé (où se trouve la limite, quelle activité est maintenue, qui sont le ou les partenaires de "repli"…);

Procédures connues de tous et disponibles rapidement (validées par la direction)

2) **Avoir prévu au préalable un SLA / une Convention :**

Il s'agit d'un document rédiger entre les partenaires potentiels qui contient les attentes et obligations des parties :

- Définition des contacts, Définition des accès
- Qui ? Direction , Stérilisation directement ?, Numéros de contact, noms des personnes de contact ?
- Prévision transport
- Contrat ?, Interne ?, Méthode de transport (emballage ? Attention ADR – réglementation du transport)
- Personnel d'astreinte ?
- Demander les preuves de validation, conformité, des cycles BD et preuves de libération(Copie des cycles).
- Eventuellement si mise à disposition de l'installation , fournir les plans de chargement autoclaves, code machines,…

Attention cela ne solutionne pas tous les problèmes car il n'y a pas de lien entre votre base de données et celle du partenaire potentiel. Faut-il envisager une intégration des données dans un autre site ? Mais hors réseau complexe …

3) **Problématique de la sauvegarde des données :**

- Faire une cartographie des technologies en réseau et hors réseau
- Analyser avec le service informatique, les différents fabricants, le fournisseur du logiciel de traçabilité les possibilité de fonctionnement hors réseau,…
- Définitions des sets d'urgences (césarienne, anévrisme cardiaque et cérébral , greffe, …)
- Avoir des backup de la base de données (rencontre du service informatique et du fournisseur de logiciel de traçabilité)
- Disposer des Compositions hors réseau (impression ? Disques durs externes ? PDF ?)
- Si nos installations peuvent travailler hors réseaux , prévoir au minimum le matériel suivant : BD ou PCD , Imprimante directe sur les machines,

- Créer un suivi des opérations urgentes
- Après l'attaque, Définir aves les différents intervenants comment réintroduire les données créées…

4) **Envisager une « valise d'urgence » comme à Rouen ?**

- Un petit guide de « je gère une procédure dégradée » (attaque informatique, coupure d'eau, de vapeur, Incendie, attentats, alerte à la bombe..) qui reprend tous les points organisationnels et les arbres décisionnels,
- Les numéros de téléphones du personnels (à jour) et des différentes hiérarchies (protégés RGPD),
- 2 téléphones indépendants du réseau (1 pour le meneur sur place et 1 pour l'interlocuteur à la direction),
- 1 Pc portable indépendant du réseau mis à jour régulièrement avec le système de traçabilité en locale (faisabilité ?), Attention aux sauvegardes ? Comment relier les données après remise de réseau ?
- Des imprimantes avec une réserve d'encre dédiée pour les étiquettes de traçabilités ? des étiquettes d'identification du set, quid des ancillaires ? Étiqueteuse à pince pour indiquer les lots ? Des Steriliners pour écrire sur les étiquettes (attention date de péremption), …
- Des rouleaux d'étiquettes (combien ?), papiers A4,
- Disque dur externe, clé USB ? Photos des ancillaires définis dans les sets urgents

5) **Ressources humaines :**

- Définir qui mène le jeu ? Définir rôle et responsabilités des acteurs impliqués avec un meneur sur place en stérilisation et sur le site de secours, un interlocuteur avec la direction et groupe de crise (pas la même personne),
- Définir (dans la mesure du possible) le besoin en personnes rappelées (volontaires souvent présents à structurer) et penser à la durée (créer des shifts si besoin),
- Repérer les compétences du service (permis camion / camionnette) et en tenir compte pour les shifts éventuels,
- Impliquer les pharmaciens et prévoir des plans de mise en place du « go/ no go » dans les procédures institutionnelles (disponibles pour tous avec quelle fonction fait quoi),
- Prévoir des mises en situation avec les acteurs concernés et les sites de repli éventuels (1 fois / an),
- Prévoir un retour à la normale (pensez à remercier les équipes et prévoir un retour sur site dans de bonnes conditions),

- Comme les attaques sont imprévues, imposer des roulements de congés des meneurs de décision (éviter l'absence prolongée de 2 preneurs de décisions en même temps) ,

« Prévoir une présence continue sur le sol territorial d'une personne connaissant les procédures »

6) **Réaliser un Débriefing final après la crise :**

- De ce qui a été et De ce qui n'a pas été et Revoir les procédures en fonction de cela ,

- Rédiger une synthèse des évènements importants pour rappel,

Et Remercier les équipes (par la Direction)

Ce document n'est qu'un support de réflexion mais une base de développement d'un projet dans le domaine.