

QU'EST QU'UN HOPITAL CYBERATTAQUÉ ?

ITW / Expert : Gilles CALMES (version Rush)

Témoignage d'un directeur de CH de référence Gilles Calmes

- ✓ M. G. Calmes, directeur du CH Sud Francilien **Séq.01**
- ✓ Hôpital de court séjour : médecine, chirurgie obstétrique (11000 lits) ... **Séq.01**
- ✓ 4000 professionnels de santé (1,3 mlns d'habitants) ... **Séq.01**
- ✓ Rappel d'évènement : du samedi 20/08 au dimanche 21/08 il y a eu une panne ... **Séq.02**
- ✓ C'est une cyberattaque, revendiquée par un mail et qu'une rançon de 10 mlns \$ est demandé. **Séq.02**
- ✓ Mise en place de plan blanc (...) **Séq.02**
- Cellule de crise : activation & organisation
- SAMU : réorientation des flux ;
- Confinement informatique ;
- Dossiers patient : reconstitution en version papier ;
- ✓ ... dans nos hôpitaux nous avons tous des plans blancs qui fonctionnent très bien. Nous sommes capables de prendre en charge (...), mais une cyberattaque, c'est quelque chose qui dure des mois et là, on est moins préparé. **Séq.09**
- ✓ On est le 21/08, 800 patients à l'hôpital, sont-ils en sécurité ? **Séq.03**
- Néonatalogie : transfert des patients par mesure de prudence ;
- ✓ ... vous avez besoin de faire un diagnostic quand un patient arrive aux urgences : l'imagerie médicale, des prises de sang, la pharmacie ... **Séq.03**
- ✓ Mise en place d'un plan de réadressage des patients (coordination avec : le SAMU, les autres établissements du territoire). **Séq.03**
- ✓ Une des grandes difficultés quand vous êtes cyberattaqué, c'est que vous ne pouvez plus communiquer ... **Séq.04**
- ✓ Le premier jour, le soir, nous avons écrit sur une feuille de papier ce qu'il c'était passé dans la journée ... **Séq.04**
- ✓ Ensuite, on a diffusé une information via les médias pour informer que l'hôpital avait été cyberattaqué ... **Séq.04**

ITW / Expert : Gilles CALMES (Post-Production)

Témoignage d'un directeur de CH de référence Gilles Calmes

Séq. 01 : Présentation générale :

- ✓ M. G. Calmes, directeur du CH Sud Francilien ;
- ✓ Hôpital de court séjour : médecine, chirurgie obstétrique (11000 lits) ... ;
- ✓ 4000 professionnels de santé (1,3 mlns d'habitants) ...

Séq. 02 : Le jour de l'attaque - Un hôpital plongé dans le noir :

- ✓ Rappel d'évènement : du samedi 20/08 au dimanche 21/08 il y a eu une panne ...
- ✓ C'est une cyberattaque, revendiquée par un mail et qu'une rançon de 10 mlns \$ est demandé.
- ✓ Mise en place de plan blanc (...)
- ✓ L'établissement était dans le noir le plus complet (...)

Séq. 03 : Réagir dans l'urgence -Les services prioritaires :

- ✓ On est le 21/08, 800 patients à l'hôpital, sont-ils en sécurité ?
- ✓ ... vous avez besoin de faire un diagnostic quand un patient arrive aux urgences : l'imagerie médicale, des prises de sang, la pharmacie ...
- ✓ Mise en place d'un plan de réadressage des patients (coordination avec : le SAMU, les autres établissements du territoire).

Séq. 04 : Communiquer en situation de crise – Informer les personnels et les patients :

- ✓ Une des grandes difficultés quand vous êtes cyberattaqué, c'est que vous ne pouvez plus communiquer ...
- ✓ Le premier jour, le soir, nous avons écrit sur une feuille de papier ce qu'il c'était passé dans la journée ...
- ✓ Ensuite, on a diffusé une information via les médias pour informer que l'hôpital avait été cyberattaqué ...

- ✓ ... et donc, progressivement, on a demandé à la population de revenir avec le fond de dossier qu'ils avaient ... **Séq.04**
- ✓ ... et le problème s'est posé aussi pour les consultations, parce que ... **Séq.04**
- ✓ ... et là, ce sont les secrétaires médicales qui sont arrivées à reconstituer une partie de leur dossier. **Séq.04**
- ✓ Il y a eu l'inquiétude parce que la population a appris que l'hôpital avait été cyberattaqué, donc vol de données médicales. **Séq.05**

- Cette cellule, qu'on a bricolé avec beaucoup de volontarisme, a fonctionné 3 semaines et permis de rassurer la population ...
- Le seul impact, c'est que, comme vos blocs opératoires sont très ralentis ...
- Travailler sous tension : les secrétaires médicales ont été fortement mis à contribution (au bout de 3 mois beaucoup ont été en burn-out) ...D'ailleurs, j'ai instauré un séminaire 1 fois/an parce que il faut reconnaître l'investissement de tous les personnels ...
- Un des responsables de sécurité du système d'information a démissionné alors qu'il n'est pour rien ...
- On a encore des coupures qui peuvent durer 4-8 h, on revient papier ...

- ✓ Ensuite, les personnels ont été inquiets parce que leurs données personnelles ... pouvaient être aussi sur le darknet. **Séq.05**
- ✓ Et donc, nous avons recensé tous les patients qui étaient venus depuis 10 ans (lettre-plante) ... **Séq.05**
- ✓ Il a fallu gérer aussi dans ce moment de communication les médias (TF1, Le Parisien) ... **Séq.06**
- ✓ Et puis, vous avez aussi les pouvoirs publics qui s'investissent (visite du ministre de la Santé, le ministre du Numérique) ... **Séq.06**
- ✓ Et pourquoi je vous parle de tout ça ? Parce que ça fait partie de la gestion de crise. Et vous êtes mobilisés aussi sur ces sujets ... **Séq.06**

- Anecdote : tout le monde a été focalisé sur la sécurité des soins et des patients pendant 2 semaines après la cyberattaque (2 cellules de crise, 3 cellules de coordination/jour, informer les personnels de ce qui peut fonctionner ou ne pas fonctionner par les documents papier et vidéo, etc.) ... Alors que des simples questions se posent : comment faire la paye ? Comment faire entrer les recettes et payer les fournisseurs ? La direction RH avait dû faire la paye de septembre

- ✓ ... et donc, progressivement, on a demandé à la population de revenir avec le fond de dossier qu'ils avaient ...
- ✓ ... et le problème s'est posé aussi pour les consultations, parce que ...
- ✓ ... et là, ce sont les secrétaires médicales qui sont arrivées à reconstituer une partie de leur dossier.

Séq. 05 : Rassurer les patients et les personnels – Les risques de fuite des données personnelles :

- ✓ Il y a eu l'inquiétude parce que la population a appris que l'hôpital avait été cyberattaqué, donc vol de données médicales.
- ✓ Les actions mises en place : numéro vert et standard patient dédié (on a demandé à des volontaires si elles étaient d'accord pour quand fasse une sorte de numéro interne.
- ✓ Ensuite, les personnels ont été inquiets parce que leurs données personnelles ... pouvaient être aussi sur le darknet.
- ✓ Et donc, nous avons recensé tous les patients qui étaient venus depuis 10 ans (lettre-plainte) ...

Séq. 06 : Communiquer avec les médias :

- ✓ Il a fallu gérer aussi dans ce moment de communication les médias (TF1, Le Parisien) ...
- ✓ Et puis, vous avez aussi les pouvoirs publics qui s'investissent (visite du ministre de la Santé, le ministre du Numérique) ...
- ✓ Et pourquoi je vous parle de tout ça ? Parce que ça fait partie de la gestion de crise. Et vous êtes mobilisés aussi sur ces sujets ...

Séq. 07 : Quel organismes contacter en urgence :

- ✓ Il y a un organisme qui s'appelle l'ANSSI (Agence National de Sécurité) ...
- ✓ Vous devez aussi informer aussi la CNIL ...
- ✓ Et puis ensuite, il y a un organisme qui ressemble à une sorte de GIGN du numérique qui s'appelle le C3N (le Centre de Lutte Contre les Attaques Numériques).

Séq. 08 : Réparer ou reconstruire :

- ✓ Lorsqu'un établissement hospitalier est confronté à une cyberattaque, il a deux options. Soit il décide de réparer le système d'information ...

avec papier et crayon (NB : ça représente 5000 agents, d'ailleurs, on avait dû négocier avec l'assurance Maladie une avance ...

- ✓ Il y a un organisme qui s'appelle l'ANSSI (Agence National de Sécurité) ... **Séq.07**
- ✓ Vous devez aussi informer aussi la CNIL ... **Séq.07**
- ✓ Et puis ensuite, il y a un organisme qui ressemble à une sorte de GIGN du numérique qui s'appelle le C3N (le Centre de Lutte Contre les Attaques Numériques). **Séq.07**

- ✓ Les actions mises en place : numéro vert et standard patient dédié (on a demandé à des volontaires si elles étaient d'accord pour quand fasse une sorte de numéro interne. **Séq.05**

→ Retour au début (24h Time Code) : ...

- ✓ Lorsqu'un établissement hospitalier est confronté à une cyberattaque, il a deux options. Soit il décide de réparer le système d'information ... **Séq.08**
- ✓ Nous, nous sommes sur un territoire en Essonne où le seul établissement de recours, c'est le CHSF. **Séq.08**
- ✓ Donc nous, on a décidé de réparer. Ça nous a pris 3 mois ... **Séq.08**
- ✓ D'autres hôpitaux qui se trouvent sur des territoires où il y a + d'établissements ... **Séq.08**
- ✓ Les 6 phases d'une cyberattaque : 1) Détection de la panne, 2) Confirmation de cyberattaque, 3) Confinement de SI (les systèmes d'information), 4) Diagnostic, 5) Réparation de système, 6) Reconstruction. **Séq.08**
- ✓ Alors, les premiers enseignements immédiats à chaud, au bout de 2, 3, 4 semaines... Parce qu'après, il y a des enseignements bien plus conséquents qui se font dans le temps. **Séq.08**
- ✓ Tout d'abord, nous devons disposer dans nos établissements de santé d'une cartographie des risques numériques. **Séq.08**
- ✓ Se préparer : 1) Cartographier les risques numériques, 2) PCA (Plans de Continuité de l'Activité) et PRA (Plans de Reprise de l'Activité) sur papier, 3) Annuaire sur papier, 4) Définir des procédures RH et fournisseurs. **Séq.08**

- ✓ Nous, nous sommes sur un territoire en Essonne où le seul établissement de recours, c'est le CHSF.
- ✓ Donc nous, on a décidé de réparer. Ça nous a pris 3 mois ...
- ✓ D'autres hôpitaux qui se trouvent sur des territoires où il y a + d'établissements ...
- ✓ Les 6 phases d'une cyberattaque : 1) Détection de la panne, 2) Confirmation de cyberattaque, 3) Confinement de SI (les systèmes d'information), 4) Diagnostic, 5) Réparation de système, 6) Reconstruction.

Séq. 09 : Les premiers enseignements :

- ✓ Alors, les premiers enseignements immédiats à chaud, au bout de 2, 3, 4 semaines... Parce qu'après, il y a des enseignements bien plus conséquents qui se font dans le temps.
- ✓ Tout d'abord, nous devons disposer dans nos établissements de santé d'une cartographie des risques numériques.
- ✓ Se préparer : 1) Cartographier les risques numériques, 2) PCA (Plans de Continuité de l'Activité) et PRA (Plans de Reprise de l'Activité) sur papier, 3) Annuaire sur papier, 4) Définir des procédures RH et fournisseurs.
- ✓ ... dans nos hôpitaux nous avons tous des plans blancs qui fonctionnent très bien. Nous sommes capables de prendre en charge (...), mais une cyberattaque, c'est quelque chose qui dure des mois et là, on est moins préparé.