JIB

CYBERATTAQUES ET CYBERSECURITE :QUE DOIVENT SAVOIR LES BIOLOGISTES MEDICAUX EN 2023 ?

Récit d'une cyberattaque

Hôpitaux Nord-Ouest
Villefranche sur Saône

Laurence MOULY
Chef de Service du Laboratoire de Biologie Médicale

Nasser AMANI
Directeur des Services Numériques du Territoire

Le GHT Rhône Nord Beaujolais Dombes

6 Etablissements

10 EHPAD

3138 Lits et places

200 726 Consultations

100 000 Passage aux U

443 Médecins

4247 Personnels

337 000 habitants **2** départements

Un Système d'Information Unique

DSN Unique

+ de 60 Applications

450 Serveurs

3 000 Postes de travail

Indicateurs HNO Villefranche/Saône

Etablissement support du GHT

450
Lits MCO

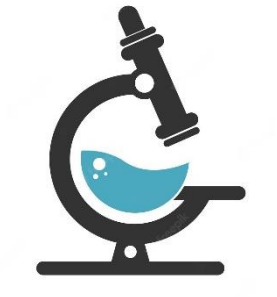
12 000
Interventions Chirurgicales

2 000
accouchements

Urgences adultes et pédiatriques

Réanimation

LABORATOIRE



- 1 seul laboratoire sur le GHT
- Polyvalent avec dépôt de sang
- 30 000 millions B/an (800 dossiers jours (hors COVID))
- 6,4 ETP biologistes dont une assistante + 1 interne
- 36 ETP techniciens de laboratoire
- Petite activité de prélèvement

Cyberattaque du 15/02/2021

Contexte

Vacances scolaires = effectif réduit

Début de la 3ème vague COVID

2 mois après un changement de SIL (GLIMS)

1 semaine après la cyberattaque de l'hôpital de DAX

Chronologie des 24 premières heures

15-02-2021 4h30 : Déclaration d'un incident informatique

- Appel du service d'Urgences déclarant une panne du système d'information de gestion des urgences
- Analyse de la panne et constat d'un incident majeur de sécurité (chiffrement massif des serveurs, postes de travail et des données)

Panne constatée par le technicien de garde : appel de l'astreinte informatique

→ incident majeur sans précision, **consigne d'éteindre tous les PC**

→ Appel du biologiste d'astreinte

15-02-2021 4h50 : Appel du directeur de garde

- Mise en place de la procédure de confinement total du système d'information :
  - Arrêt du SI (dont la téléphonie) et de toutes les liaisons vers l'extérieur
  - Passage en mode dégradé
  - Analyse des impacts sur notre SI

Chronologie des 24 premières heures

15-02-2021 6h30 : Déclaration d'incident de sécurité

- Direction Générale
- ARS – Régulation SAMU
- Cert FR (Computer Emergency Response Team) - CNIL

= ANSSI (Agence Nationale de Sécurité des Systèmes d'Information)

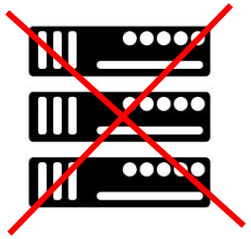
15-02-2021 7h38 : sms de la DG

Bonjour
Nous faisons l'objet d'une très sérieuse attaque virale sur l'ensemble des sites HNO. Nasser et ses équipes sont sur le terrain pour tout couper afin d'arrêter la propagation. SAU, laboratoire et imagerie fonctionnent en mode dégradé. Il n'y a plus d'accès au DPI Easily, ni messagerie, ni téléphonie.
Il ne faut pas redémarrer les PC. A plus tard.

Chronologie des 24 premières heures

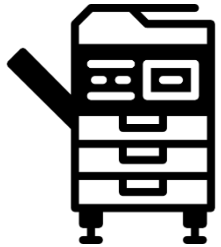
Constat : sidération

CE QU'ON A PAS



CE QU'ON A

Des automates en état de marche



Une unique photocopieuse fonctionnelle ne nécessitant pas de connexion d'un opérateur HNO

Une équipe de battants

CENTRE HOSPITALIER
Dax-Côte d'Argent

L'expérience de DAX : ça va durer longtemps !

Chronologie des 24 premières heures

Actions immédiates

Prévenir les services de prélever le strict nécessaire
S'en tenir à la Liste des examens urgents
Prévenir l'EFS : transfusions sans informatique = transfusions en O
Rappeler la procédure d'enregistrement manuel des demandes
Organiser le rendu des résultats papier (de l'automate au service avec validation biologique sur résultat de l'automate)
Retour au papier / crayon !

Imprimantes automates souvent reliées au réseau
Comptes rendus automate souvent incompréhensibles avec peu d'informations concernant le patient
Pas de valeurs normales
Pas de fax, pneumatique uniquement relié à la réanimation/urgences

Chronologie des 24 premières heures

15-02-2021 12h30 : 1ère Cellule de crise (J0)

- DSNT
  - Etat des lieux de la situation :
    - Confirmation de Cyber Attaque Totale impactant le « cœur de notre système d'information »
    - Système de sauvegarde intègre
    - Pas de trace d'extraction de données
    - Aucune durée d'indisponibilité ne peut être donnée

- Labo
  - Tous les automates fonctionnels (sauf électrophorèses) mais nécessité de connecter des imprimantes en directe
  - Plus de serveurs de résultats : nécessité de mettre en place un système de coursiers pour acheminer les résultats aux services

Chronologie des 24 premières heures

15-02-2021 18h30 : 2ème Cellule de crise (J0)

- DSNT
  - Confirmation que le Système de sauvegarde est intègre
  - Rétablissement de la téléphonie qui n'était impactée
  - *« Nous allons engager une restauration de l'ensemble du Système »*
  - La durée de la panne est incertaine
  - Les équipes de l'ANSSI sont en route afin de nous accompagner (10 personnes)

- Cellule de crise
  - Déprogrammation d'une partie des interventions chirurgicales
  - Fermeture des urgences aux SAMU et Pompiers
  - Les patients en présentation spontanée au SAU sont pris en charge
  - Maintien des patients stables des services critiques

J1

16-02-2021 10h00 : Conférence de presse

- Volonté de transparence sur l'incident
- Médiatisation de l'incident
- Enquête ouverte par le parquet de Paris

16-02-2021 12h00 : 3ème Cellule de crise

- DSNT
  - Le Système d'Information doit être intégralement reconstruit
  - Démarrage de la phase de remédiation
- La Cellule de crise déterminera les priorités (PCA, PRA…)
- Laboratoire
  - Plus d'espoir que cette crise soit résolue rapidement
  - Plusieurs semaines pour récupérer la totalité des nos logiciels
  - Prioriser la récupération du middleware

J2

- Interdiction de démarrer les PC, analyse des postes en commençant par ceux de MPL, des automates puis Myla
- **Etiquettes de dégradé** : demande à MIPS de faire imprimer des étiquettes par un autre site (10000 supplémentaires ?)
- **Filière urgences/réa** : mise en place de feuilles de dégradé roses avec transmission directe du prélèvement aux techniciens du prélèvement
- Suivi des **températures** : surveillance toutes les 4 heures des enceintes et installation de POD dans les enceintes du dépôt
- **Gestion de stocks** : pas de retour de GesStock annoncé avant longtemps
  - Tableaux de déstockage dans tous les secteurs dès le début, stock visuel et commandes par fax
  - Cahiers de traçabilité des commandes et des déstockages à partir du 16/02 J1
- **Maintenances** : mettre en place des cahiers de suivi aux différents postes
- **Sauvegardes** : problèmes des sauvegardes automatisées sur le réseau, possible sur clé si les PC ont été contrôlés.

J2

- **Immuno-hématologie et transfusion** : réalisation des groupages et RAI pour transfusions, délivrance par dépôt uniquement pour les urgences sinon délivrance et traçabilité par l'EFS.
- Retour de la **bactériologie avec papier**, reprise de nos fiches Scanbac.
- Sérologies : portoirs avec les tubes en attente. Réalisation des sérologies toxoplasmoses toutes les 48h. Ag HBs urgents et autres urgences au coup par coup.
- Mouvements de patient : appeler les urgences pour les patients passés par les urgences depuis le 15/02 sinon listing des services distribué au laboratoire.
- **Consultations externes** : récupération du fichier des rendez-vous, annulation des rendez-vous jusqu'au mercredi de la semaine suivante
- Formats de résultats : en fonction de la reprise de MPL voir comment améliorer le rendu en biochimie/hémostase/hématocytologie
- Problématique du **suivi des CIQ** gérés que sur le middleware

Et les jours suivants :

- Gestion des non conformités
- Elargissement des analyses réalisées
- Reprise de la sous-traitance

La remédiation du système d'information

REMEDIATION

J0 — Réanimation Néonatologie J3 — Urgences J10 — Plateaux Médico-Technique A partir de J10 — Activité normale > 7 semaines

⇨ Relance progressive et séquencée de tous les services et établissements
⇨ Priorisation définie par la cellule décisionnelle

RETOUR (TRES) PROGRESSIF

J0 — Quelques PC J4 — Middleware J8 — SIL J13 — Activité normale > 1 mois

Les principaux enseignements
ce qui a bien fonctionné

- Cellules de crises de gestion de l'incident,
- La poursuite de l'activité dans les services de soins et médico-techniques en mode dégradé même si ce mode s'est parfois révélé inadapté,
- Réactivité et investissement des équipes IT HNO, prestataires informatiques et bio-médicaux,
- Mode Hybride d'hébergement de nos applications (DPI, RH),
- Stratégie de reprise d'activité et de redémarrage des applications au cœur du processus de soins connue et maitrisée,
- Soutien, Collaboration, Solidarité, Entraide au sein de l'équipe IT, et aussi avec l' ensemble des professionnels de chaque établissement,
- Communication externe et transparence sur l'incident rencontré

Les principaux enseignements
ce qui a manqué ou pas fonctionné

- Difficultés pour téléphoner et communiquer le premier jour alors que la communication est essentielle en début de crise
- Absence d'annuaire papier à jour et connu de tous

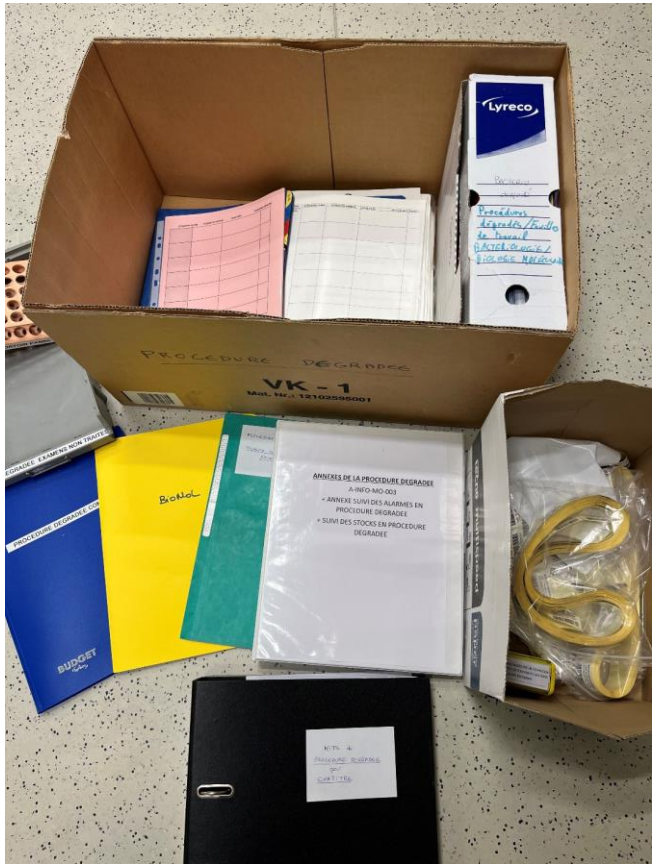
- « Tendance » au sans papier

- Temps nécessaire pour la mise en place d'une organisation efficiente

- Les procédures dégradées n'avaient pas été conçues pour des pannes de cette ampleur ni de cette durée (exemple : nombre d'étiquettes insuffisant, bactério sans papier, résultats de biologie moléculaire…)

Les principaux enseignements
au laboratoire

- Ça n'arrive pas qu'aux autres !
- Importance de la mise en place rapide d'une cellule de crise : communication ++
- Garder les versions papiers de certains documents essentiels
- Ne pas connecter l'ensemble des photocopieuses sur le réseau !
- Tester les procédures dégradées aux changements de version des logiciels
- Etre prêts :
  - Check-list de mise en place
  - Avoir un kit « dégradé » prêt à être utilisé
  - Entrainements
  - Retour d'expérience/réunions en cas de pannes réseaux



La doctrine du Management de la sécurité des HNO

Utilisateurs du SI
Equipes IT
Exercice Cyber

Pilotage Direction générale
Cartographie
Analyse des risques
Politique de sécurité
Audit de sécurité

Cloisonnement/ filtrage
Antispam
Compte Admin
Authentification et droits d'accès
Accès distant
Sécurité physique et environnemental

Détection et journalisation
Réponse aux incidents
Traitements des alertes
Corrélation et analyse des journaux

Gestion des crises
PCA / PRA
Communication

JIB

Merci de votre attention !