CENTRE HOSPITALIER
Dax-Côte d'Argent

Cyberattaque au CH de DAX
RETEX un an après la crise

@chdax

Le 9 février 2021, Le Centre Hospitalier de Dax faisait l'objet d'une cyberattaque « anéantissant » son système d'information.

Ce retour d'expérience à date anniversaire, a été réalisé afin de faire prendre conscience des impacts concrets d'une telle attaque sur les missions essentielles d'un centre hospitalier, sur l'accueil et la prise en charge des patients, sur les organisations et les équipes qui y travaillent.

Plus d'un an après, si le cyclone et la tempête sont dernière nous, il reste des stigmates forts, et le Centre Hospitalier est loin de naviguer sur une mer d'huile.

Cyberattaque: *« quand un hôpital essuie un cyclone »*

- L'œil du cyclone : le jour J
- La tempête : comment fonctionner en mode dégradé ? *(1 semaine)*
- La houle : une lente remontée *(3 mois)*
- Vers une mer plus calme ? *(encore quelques mois… une année…)*

L'œil du cyclone : jour J

9/02/21 : 2h du matin

- Standard isolé, téléphonie bloquée, informatique bloquée
- L'informaticien d'astreinte ne peut rien résoudre et appelle le RSSI
- Directeur d'astreinte réveillé par le RSSI : situation très critique
- Aucun accès informatique, absence de téléphone, des patients présents et d'autres qui arrivent aux urgences

Au petit matin: confirmation d'une cyberattaque massive:

- Cryptolocker : chiffrage de la majorité des serveurs (85% soit 150 serveurs), l'accès au réseau impossible, les sauvegardes chiffrées
- Appel à l'ANSSI et Orange Cyber Défense pour circonscrire l'attaque
- Mise en alerte des SAMU 40/64 et de la médecine de ville pour limiter les flux aux urgences
- Le Directeur venant de muter, le Directeur intérimaire est prévenu ainsi que l'ARS
- Mobilisation générale pour un passage en procédures dégradées

L'œil du cyclone : jour J

13h30 : 1ère cellule de crise SIDERATION

- Aucun moyen de communication (téléphone, mails, annuaires…)
- Plus aucune information sur les patients, plus de prescription, aucun historique d'image, de labo… reste la mémoire humaine, et le papier
- Mais tous les services d'hospitalisation ne disposent pas du DPI et le dossier papier est encore très présent
- Plus de stérilisation, imagerie mais sans possibilité de stocker les images, résultats de labo sur les automates
- Arrêt total de la radiothérapie, du logiciel de chimio, Drugcam
- Plus de plans de lits, plus d'étiquettes patient, aucun planning de RV patient
- Plus aucun applicatif métier : gestion RH, planning, GAP, GEF ……

⇒ Prise en conscience d'un arrêt total qui va durer (X semaines, X mois????) et du risque pour les patients (perte de chance)

Enseignement: Une cyberattaque dépasse une simple crise informatique

L'œil du cyclone : jour J

Mesures prises : Mise en place de procédures dégradées

- Dans les services, retour au papier/crayon pour la gestion des patients et les prises en charge, (prescriptions, traçabilité, CR, plans de lits) retour aux panneaux Véléda dans les services
- Echange des 06 personnels pour communiquer en interne et diffusion d'une liste papier des téléphones utiles
- Matériel biomédical déconnecté du réseau pour protection
- Chaque service s'organise en autonomie pour assurer les prises en charge
- Demande de limitation des prescriptions au laboratoire : résultats en 5h au lieu d'1h, CR incompréhensibles et mise en place d'un manuel de concordance des codes, obligation de doubler les astreintes de nuit. Arrêt des consultations externes
- Imagerie : lecture directement sur 1 seule console, pas de stockage des images, CR rédigé papier, garde sur place car pas de télé imagerie. Arrêt des consultations externes

Enseignement : où l'intelligence collective et la débrouillardise permettent de « sauver les meubles »

La tempête (1ère semaine)

Obligation: Reconstruire une nouvelle infrastructure réseau/serveurs avant de remettre en service les applications et de récupérer les données (si elles sont récupérables?)

Nouvelles mesures prises :

- Enregistrement administratif des patients : manuel
- Consultations : à l'aveugle car absence d'agendas
- Radiothérapie à l'arrêt : contacts avec d'autres centres pour assurer l'accueil des patients; organisation en 48h des transferts et les 3 radiothérapeutes qui suivent les patients (Bordeaux, Pau, Bayonne)
- Pharmacie : formulaires de commande « papier », logiciel de chimio non opérationnel mais l'isolateur fonctionne : fiches de fabrication manuelle mais 20 préparations possibles au lieu des 80, proposition d'aide du CH de Mont de Marsan
- Stérilisation : aucune libération de lots car absence de traçabilité : déprogrammation au bloc (maintien des urgences uniquement)

Enseignement: 30 ans d'informatisation anéantis n'empêchent pas un sursaut du collectif

La tempête (1ère semaine)

- Distribution et Installation de PC et clé 4G pour les secrétariats, cadres, fonctions administratives : assurer le minimum vital (admissions des patients, étiquettes, CR, commandes fournisseurs …) et autorisation d'utilisation de PC portables personnels
- Mise en place d'adresses mails temporaires
- Mise en place de groupes WhatsApp pour communiquer et centraliser les besoins de renfort (redéploiement des personnels administratifs/médico-tech ne pouvant plus travailler) et mise en place d'une équipe de coursiers internes qui distribuent les papiers (examens, plans de lits, CR …)
- Transports : plateforme indisponible, bons manuels et appels téléphoniques
- Encadrement : gestion des plannings « papier »
- Paye de février assurée (virement identique à janvier par le Trésor Public)

Enseignement: Où le système D l'emporte sur le hiérarchique et les fonctionnements classiques

La tempête

Gestion institutionnelle :

- Mise en place d'une cellule de crise journalière : point de situation à la mi-journée (informatique, organisation, évaluation service par service), seul canal d'information pendant plusieurs semaines
- CR « papier » réalisé en temps réel par la DQGR et distribué dans les 2 heures dans les services

⇒ Synthèse des pb et de leur résolution, analyse des nouvelles difficultés, résolutions

- Gestion médiatique complexe avec de multiples sollicitations et une communication ciblée vers le grand public pour une meilleure gestion des flux, volonté de transparence
- Percuté par l'organisation de visites officielles (DG ARS, politiques locaux, puis visioconférence avec le Président de la République)

Enseignement : garder son sang froid, tout le monde sur le pont et à son poste

La houle, une lente remontée

Informatique: Aide capitale de l'ANSSI pour retrouver 30 ans d'informatisation

- ANSSI très présente ainsi que Orange Cyberdéfense (Prestataire de Réponse à un Incident de Sécurité)
- Cœur de confiance (active directory) rétabli en 10 jours mais (re)construction d'une nouvelle infrastructure : départ de zéro.
- Confirmation de l'absence de vol de données
- Mise en place d'un nouveau mode d'administration : durcissement
- Sauvegardes partiellement cryptées : 1ères interventions du prestataire DATABACK, sauvegardes bandes disponibles, incomplètes mais les données patients présentes (grand soulagement), quid des données administratives ?
- Remontées très lentes des données cryptées
- Création de micro-réseaux pour un fonctionnement minimal en mode restreint et isolé : accès en visu au DPI sur quelques postes (imagerie, chimio, laboratoire, stérilisation, GRH)

Enseignement: Ne pas hésiter à s'appuyer sur les compétences d'experts

La houle, une lente remontée

Une solidarité capitale :

Pour du prêt de matériel (170 PC pour remplacer l'ensemble des postes clients) et mise à disposition de compétences informatiques, et médicales (gardes en imagerie) :

- Des Centres Hospitaliers (Mont de Marsan, Bayonne, Pau, Tarbes, Lourdes, Lannemezan)
- Mairie de DAX, Conseil Départemental, de l'ALPI (Agence Landaise Pour l'Informatique), de la CCI
- Orange (prêt clés 4G)
- Fournisseurs (dons d'agendas papiers)

Enseignement: une solidarité des collègues et des partenaires qui permet de se sentir moins seul

La houle, une lente remontée

Dans les services:

- Mise à dispo en visu du DPI sur quelques postes en libre service (AMA, médecins), Terminal Urgences aux urgences mais sans aucune interface
- Réinstallation progressive en radiothérapie sur serveur isolé, déclaration à l'ASN et inspection
- GRH et GTT remontées sur quelques postes : travail de rattrapage (paye exacte sur avril), messagerie et accès internet
- Imagerie : recherche d'aide pour assurer les gardes *:* aide des radiologues du CH Côte Basque et relance du PIMM pour télé interprétation
- Remontée CITRIX pour les utilisateurs fin mars mais très partiel et progressif : Administration, site MCO puis sites annexes (terminé fin mai)
- Angoisse : récupération de la base de données GAP et GEF; base GAP remontée partiellement fin avril

Enseignement : apprendre la patience

La houle, une lente remontée

Gestion institutionnelle :

- Mise en place du Comité de Reprise d'Activité pour élaborer le Plan de Reprise d'Activité (PRA) : DSIO + COMDIR + PCM + DIM; réunion hebdo afin de prioriser la remontée des briques fonctionnelles

- Priorité posée : la prise en charge du patient (TU/DPI/GAP/agendas/radiothérapie/chimio/anapath/imagerie/laboratoire)

  En tenant compte des possibilité techniques

Enseignement : des priorisations pas toujours bien expliquées et bien comprises

Vers une mer plus calme?

Été 2021

- L'essentiel est a été retrouvé et partiellement remonté : DPI pour l'accès aux documents mais pas de prescriptions informatisée, TU, GAP, radiothérapie, chimio, imagerie, labo, anapath, (mais certaines interfaces et liaisons ne sont pas opérationnelles), anesthésie, dossiers individuels (mes documents), agendas, GED fin août.
- Bascule sur le nouveau système des domaines gérés sur des serveurs autonomes
- Mais toutes les fonctionnalisées ne sont pas retrouvées (ex : prescriptions informatisées sur 3 services uniquement) et beaucoup d'instabilités et de lenteurs
- il reste encore : Bloc, GEF (clôture 2020 faite fin juin et rattrapage colossal), dictée numérique, historique des mails, contacts Outlook, hémovigilance …
- Récupération proche de 100% des données mais encore beaucoup de travail notamment avec les éditeurs pour un retour à la normale.

Enseignement : s'inscrire dans un temps long

Vers une mer plus calme?

Été 2021

- Perspectives : encore des semaines de travail, de patience et surtout un effort colossal pour rattraper 4 mois d'informations patients et les données des applicatifs administratifs (5 mois) :

  GAP-DPI-PMSI : + 30 000 dossiers à réintégrer et les mouvements

  GEF: 22 365 lignes de commande, 99 201 lignes de sortie de stock,

  5 754 lignes de paiement

  Rétrocessions 1100 lignes

  Molécules onéreuses 1080 lignes

  Et un énorme travail sur la qualité des fichiers

- Recrutements de renfort pour réintégrer les données papiers : 8 ETP
- Recours à un prestataire extérieur pour la facturation des dossiers patients

Enseignement : ne pas sous estimer le travail de rattrapage pour ne pas handicaper l'avenir

Vers une mer plus calme?

A un an

- Certains applicatifs non compatibles avec l'évolution de l'infrastructure réseau, ex : logiciel de bloc, logiciel d'écho anténatale = changement
- Des solutions toujours instables ou partiellement opérationnelles, ex : dictée numérique
- Des briques pas encore accessibles : logiciel d'hémovigilance et liaison EFS logiciel de télémédecine, logiciel de radioprotection, logiciel qualité du laboratoire, mails antérieurs à l'attaque, contacts Outlook, logiciel de suivi des prestations hôtelières, certaines interfaces et liaisons (ex DMP, PAACO)
- Des fonctionnalités dans le domaine biomédical non remontées , ex : EEG/gravure CD, applicatif Nexus (don d'organes/téléAvc)
- Rattrapage non terminé, clôture 2021 non réalisée

Enseignement : complexité et grande diversité de nos applicatifs

Vers une mer plus calme?

Impact financier à un an:

- Investissements : 174 000 € (matériel pour reconstruction du réseau)
- Prestations cybersécurité et réinstallations : 546 000€
- Sous-traitance biologie : 9 000€
- Coût RH (PM et PNM) renforts, heures sup : 1 484 000€
- 143 000€ pertes de recettes commerciales

Au total 2 356 000€, compensés par l'ARS

Manque de recettes liées à l'activité (radiothérapie/imagerie/laboratoire) estimés à 2 344 000 € et problématique de trésorerie (40 M d'€) neutralisée **mais** couvertes par la garantie de financement liée au Covid.

Enseignement : Impact financier important (1,5% du budget) et les pouvoirs publics au rendez vous

Quelques enseignements …

- Une gestion de crise marathonienne : des semaines, des mois, un an… et peut-être plus.
- Peu de lisibilité et de certitudes pendant tous ces mois
- Choc traumatique certain, fatigue cognitive et physique renforcée par la 4ème et 5ème vague Covid
- Des équipes sursollicitées surtout la DSI, les services médico-techniques, toujours présents mais « rincés »
- Une sortie de crise et la perspective d'un retour à la normale excessivement long

« quand la ligne d'horizon recule au fur et à mesure que l'on avance »

- Prise de conscience de notre vulnérabilité numérique (les anciens plus agiles que les jeunes ?) et de l'obligation d'investir dans la sécurité informatique (compétences, investissements, prestations sécurité…)
- Un système d'information renforcé, des règles de sécurités encore plus fortes
- Un accélérateur de déploiement des solutions (sécurité/ évolution des versions..)

Mais …

Quelques enseignements …

Une aventure humaine incroyable

Engagement

Solidarité

Agilité

Créativité

Collaboration et la responsabilité de tous

une force pour le futur

Verbatim recueilli à l'occasion du retex interne

« Les équipes ont fait preuve de réactivité, de courage, de solidarité, de sagesse, de volontariat, d'engagement au prix d'une grande pression, d'une grande fatigue cognitive, physique et psychique » Responsable PUI

« Notre fonctionnement est intimement lié à l'informatique dans tous les domaines de nos pratiques soignantes et logistiques, ce qui nous rend vulnérable » Cadre de Santé maladie infectieuse

« La cyberattaque a été un levier déterminant pour la santé et l'hygiène du SI » DSIO

« L'évènement le plus impactant de l'histoire de notre établissement » Chef de service Urgences

« *Cela a montré la résilience d'un établissement et de ses services, sa capacité à s'entraider, à faire face, à développer de l'adaptabilité »* Faisant Fonction de Cadre pédopsychiatrie

« Avoir pris conscience de la complexité d'un système informatique et de sa remise en route » Cadre pédiatrie

« Importance de conserver 2 supports, informatique et papier » Attachée gériatrie

« Ne pas paniquer et s'adapter, on a su réagir vite et développer la communication informelle … et s'échanger des astuces » IDEC obésité

« *Une impression générale de quelque chose de terrible qui est derrière nous »* Cadre assistant social

« Miser sur le talent personnel, la capacité à réfléchir vite et bien, la volonté de tous à apporter sans réserve l'aide demandée » Laboratoire

Aline Gilet-Caubère, Directrice Qualité Gestion des Risques, relations usagers, communication (version du 18 mars 2022)
Contact : communication@ch-dax.fr