Webinaire de sensibilisation à la cybersécurité

Etablissements de santé

Mardi 5 avril 2022

Sommaire

1. Propos introductifs du DG ARS ARA
2. Rappel de la feuille de route confiée à l'ARS
3. Gendarmerie nationale
4. Etude de cas : retour d'expérience de 3 cyberattaques
5. Questions / Réponses
6. Conclusion

Propos introductifs du DG ARS ARA

Propos introductifs

Mesdames, Messieurs,

Les incidents de sécurité des systèmes d'information déclarés par les établissements de santé sont en constante évolution. Les gisements de données de santé sont ouvertement la cible de ces tentatives d'extorsion.

En 2021 le nombre d'incidents SSI déclarés en France a doublé par rapport à l'année précédente et 2 fuites importantes de données médicales se sont produites. La région ARA n'a pas été épargnée : 60 signalements nous ont été remontés en 2021. Les conséquences sont importantes sur l'organisation et la sécurité des soins et des directeurs d'établissements et des professionnels de santé qui en ont été victimes vont en témoigner dans quelques instants.

En 2022 le risque de cyberattaques est amplifié en raison de la guerre en Ukraine.

Des bases concrètes de sécurité des systèmes d'information ont déjà été posées et prises en compte de manière notable par les établissements de santé, notamment de la région. Pour autant les systèmes d'information des établissements restent vulnérables et nécessitent le renfort de nos actions et la mise en œuvre de dispositions autant techniques que pédagogiques.

Propos introductifs

La volonté politique est forte pour faire face aux défis qui s'imposent à nous.
Le Président de la République a annoncé des nouvelles mesures le 18 février 2021 ; nouvelles mesures qui ont été fixées dans une feuille de route dont la supervision de la mise en œuvre est confiée aux ARS.

Je souhaite que ces mesures soient déclinées en région Auvergne-Rhône-Alpes de manière collégiale, pragmatique et efficace.

Les actions à mener sont principalement à la charge des établissements, pour autant, l'agence contribuera à leur mise en place, notamment :

en soutenant les projets d'investissements nationaux aidant financièrement les établissements, et
en structurant une démarche régionale rassemblant les acteurs spécialisés du domaine de la sécurité des SI.

Le défi est de taille, nous le savons, mais il est essentiel/indispensable que la sécurité des systèmes d'information devienne une priorité au même titre que d'autres et que vous lui consacriez l'appui et les moyens nécessaires.
Je sais pouvoir compter sur votre engagement, et l'agence vous accompagnera dans toute la mesure du possible.

Je vous remercie.

Rappel de la feuille de route ARS
« Plan de renforcement de la cybersécurité des établissements de santé »

Des actions déjà engagées par les ES

- Instruction du 14/10/**2016** **imposant** à tous les ES un **plan d'action Sécurité SI** à 6-12-18 mois
- La **SSI est une exigence posée comme prérequis** depuis **2017** à travers les programmes
  - Hôpital numérique (>100 ES)
  - HOP'EN (>200 ES)
  - **SUN-ES en cours**

  A travers lesquels les ES doivent
  - Désigner un **Responsable Sécurité** des SI
  - Rédiger un **Plan de Reprise d'Activité** prévoyant le passage en **mode dégradé**
  - Rédiger une **Politique Générale de Sécurité** SI incluant **analyse de risques et plan de traitement**
  - Faire réaliser des **audits d'intrusion**, …
- **2020** : Désignation des **15 ES supports de GHT** comme **Opérateurs de Services Essentiels** (OSE) impliquant un parcours sécurité en lien avec l'ANSSI puis une déclinaison dans leur GHT

→ Prise en compte notable de la sécurité SI par les établissements sanitaires en ARA

Le plan de renforcement demandé

Le MSS a lancé en juillet 2021 un plan d'actions définissant les mesures prioritaires à mener par les ES et en a confié la déclinaison territoriale et le suivi aux ARS :

- Sensibiliser aux risques cyber (formation, …)
- Fédérer des actions collectives (guides, outils, appui, …)
- Structurer les réponses aux incidents (gestion de crise, ressources externes, …)
- Vérifier l'avancement et s'assurer de la réalisation des mesures clés (PCA/PRA)

En dernière partie, des pistes de travail vous seront proposées…

Gendarmerie nationale

Colonel Yoni Forest

Présentation de la menace

Colonel Yoni Forest

Typologie de la menace

Définition :

« tentative d'atteinte à des systèmes d'information réalisée dans un but malveillant. Elle peut avoir pour objectif de voler des données (secrets militaires, diplomatiques ou industriels, données personnelles bancaires, etc.), de détruire, endommager ou altérer le fonctionnement normal de systèmes d'information (dont les systèmes industriels) »

ANSSI

Auteurs :

- 20 % cybermafias (dvmt de propres outils)
- 26 % groupes de pirates
- 26 % cybercriminels (achat de service de piratage)
- 17 % de script kiddies
- 8 % de collaborateurs internes

Cibles :

- ordinateurs, serveurs, isolés ou en réseaux reliés ou non à internet
- équipements périphériques
- appareils communicants (TPH, tablettes…)

4 types de risques cyber :

- piratage
- atteinte à l'image
- espionnage
- sabotage

Secteurs ciblés fonction de :

- dépendance à l'automatisation et au numérique
- retard en matière de cyber-résilience
- insuffisance dans les procédures type PCA
- conjoncture : secteur de la santé

Colonel Yoni Forest

Top 15 des cybermenaces

source ENISA

10 enseignements à retenir

1. Nouvelle phase de transformation du numérique donc nouveaux défis.
2. Dépendance accrue du cyberespace après la pandémie COVID-19.
3. Utilisation des plateformes de médias sociaux comme cibles des attaques cyber.
4. Véritable organisation du crime avec des attaques finement ciblées et persistantes sur des données de grande valeur (par exemple, propriété intellectuelle et secrets d'états) – parrainage étatique.
5. Attaques distribuées massivement avec une courte durée et un large impact pour organiser le vol d'informations d'identification.
6. Motivation financière derrière la majorité des cyberattaques.
7. Ransomware en forte augmentation avec des impacts financiers élevés.
8. Cyberattaques détectées : partie immergée de l'iceberg.
9. Dimension humaine : principal maillon de vulnérabilité.
10. Automatisation des systèmes de sécurité encore insuffisante.

CONSÉQUENCE D'UNE CYBERATTAQUE

- **Activité impactée :**

- Interruption totale ou partielle d'un élément ou de la totalité d'une chaîne logistique, de production, de gestion … en fonction du secteur d'activité.
- Interruption du site internet.
- Réallocation des moyens pour gérer la crise et donc baisse de la productivité.
- Stress et surmenage des collaborateurs.

- **Réputation atteinte :**

- Court terme (exemple cours de bourse, risque d'acquisition…).
- Moyen terme (perte de patientèles…).
- Long terme (impact de la crédibilité).

- **Risque juridique :**
- Recours en responsabilité civile voire pénale.

Pérennité de l'entité attaquée en jeu

Colonel Yoni Forest

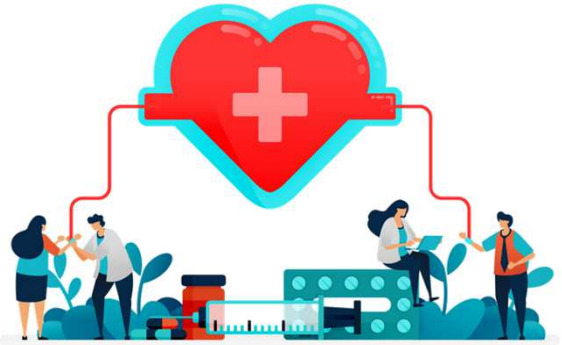
Les établissement de santé, un secteur impacté

« les hôpitaux et autres entités du secteur médico-social représentent l'une des cibles privilégiées des attaquants »

État de la menace rançongiciel – ANSSI – 01/02/2021

Pourquoi ?

 Infrastructure critique, cible naturelle en temps « normal »
 Effet d'aubaine : mise en place télétravail = augmentation de la surface d'attaque dont les conséquences avec la crise COVID19 en accroît la criticité.
 Établissements de santé et médico-social : faible niveau de sécurité numérique et milieu par définition ouvert (vulnérabilité pour intrusion également physique).



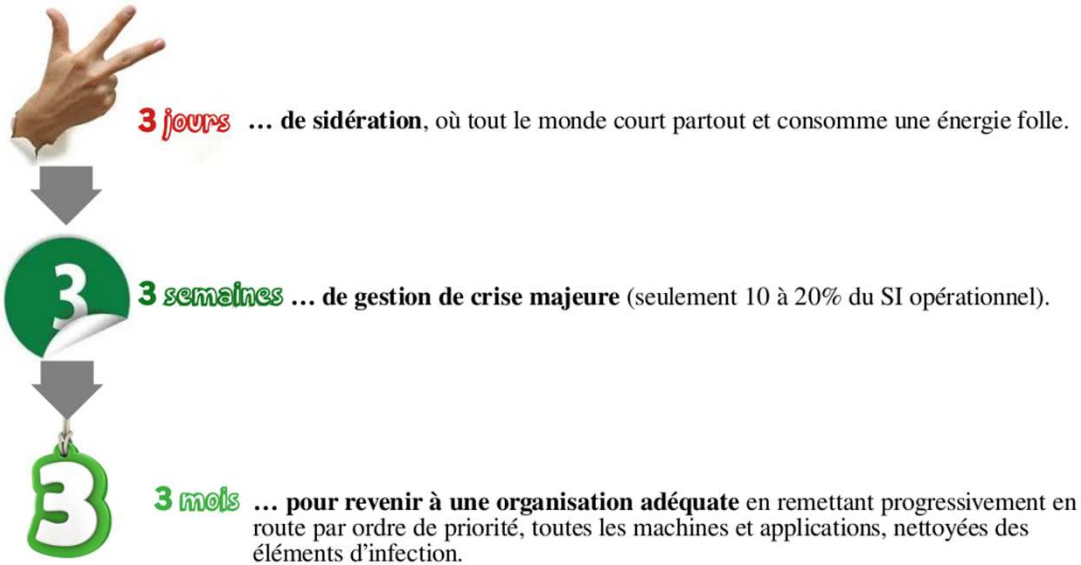
Comment ?

- 70 % des attaques = attaques par rançongiciel.
- Intensification de la menace depuis 2019.
- En 2020, 8 % des attaques par rançongiciel concernaient le secteur de la santé Avec 3 hôpitaux en ZGN.
- En 2021, la RAURA est également touchée (Villefranche sur Saône 15/02/2021) avec paralysie ou forte perturbation du site web de l'hôpital, des standards téléphoniques, de la gestion des patients avec comme conséquence notamment des déprogrammations des opérations chirurgicales.

Colonel Yoni Forest

La règle des 3x3

- **Une attaque réussie déclenche la règle des 3x3[1]**



3 jours … **de sidération**, où tout le monde court partout et consomme une énergie folle.

3 semaines … **de gestion de crise majeure** (seulement 10 à 20% du SI opérationnel).

3 mois … **pour revenir à une organisation adéquate** en remettant progressivement en route par ordre de priorité, toutes les machines et applications, nettoyées des éléments d'infection.

- « Nous avons dû formater 1500 ordinateurs et ré-initialiser 250 serveurs », explique de son côté Arnaud Mabire, vice-président de la communauté d'agglomération **Evreux Portes de Normandie**, frappée par un rançongiciel mi-décembre 2020 - environ 1,5 mois de travail.
- [1] *Gérôme Billois, associé chez Wavestone*

Colonel Yoni Forest

Organisation de la réponse

Colonel Yoni Forest

LE RÉSEAU GENDARMERIE

NATIONAL

- Centre de lutte contre les Criminalités Numériques (C3N)
- Enquêteurs en Technologies Numériques (N'Tech)

RÉGIONAL ET DÉPARTEMENTAL

- Sections de recherches – Groupes Cyber (Antenne C3N – N'Tech)
- Sections Opérationnelles de Luttes contre les Cybermenaces (SOLC - N'Tech)

LOCAL

- Correspondants en Technologies Numériques (C-N'Tech)
- Tout gendarme de terrain

Colonel Yoni Forest

LES ÉTAPES D'UNE GESTION DE CRISE CYBER
(MÉTIER VERSUS CYBER)

*SOURCE ANSSI

SIGNALER

Colonel Yoni Forest

QUI EST CIBLÉ ?

La réponse est simple : tout le monde.
Vous êtes une cible potentielle des **rançongiciels.**

- QUE VOUS SOYEZ UN PARTICULIER, UNE ENTREPRISE OU UNE COLLECTIVITÉ…
- …QUELS QUE SOIENT VOS APPAREILS…
- …ET QUELS QUE SOIENT VOS SYSTÈMES D'EXPLOITATION : iOS, Windows, Android, Linux, macOS

QUELLES SONT LES ÉTAPES DE L'ATTAQUE ?

1. **L'INFECTION** — Elle arrive principalement à votre insu quand vous ouvrez une pièce jointe ou quand vous cliquez sur un lien malveillant.
2. **LE CHIFFREMENT DES FICHIERS** — Vous ne pouvez plus utiliser votre appareil : votre système et vos applications sont bloqués et/ou vos fichiers chiffrés.
3. **LA DEMANDE DE RANÇON** — Sur votre écran, un message vous indique que vous avez été piraté et vous demande de payer une somme d'argent.

CYBERCRIMINEL

EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

BUT
Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE
Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

VICTIME

COMMENT RÉAGIR ?

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

POURQUOI NE FAUT-IL PAS PAYER ?

Même si vous réglez le montant de la rançon, rien ne vous assure que vos fichiers seront déchiffrés ou que votre ordinateur sera de nouveau accessible. De plus, vous alimentez un système et démarrez un cercle vicieux : après avoir payé, vous risquez d'être identifié comme « bon payeur » par les cybercriminels.

*SOURCE cybermalveillance.gouv.fr

Etude de cas :
retour d'expérience de 3 cas de cyberattaques en 2021

RETEX cyberattaque 25 février 2021

Frédérique Gama - Directrice

- Clinique médico-chirurgicale indépendante de 135 lits et places
- Située à proximité immédiate de Lyon (de l'autre côté de la rue)
- Chiffre d'affaires : 25 millions d'euros avec un résultat positif

Le CONTEXTE NATIONAL et REGIONAL : CYBER-ATTAQUE

➔ 10 février 2021 : Hôpital de DAX

Au niveau régional :

➔ 21 décembre 2021 : hôpital d'ALBERTVILLE

➔ 15 février 2021 : hôpital de Villefranche/Saône

➔ 25 février 2021 : hôpital de Saint-Etienne

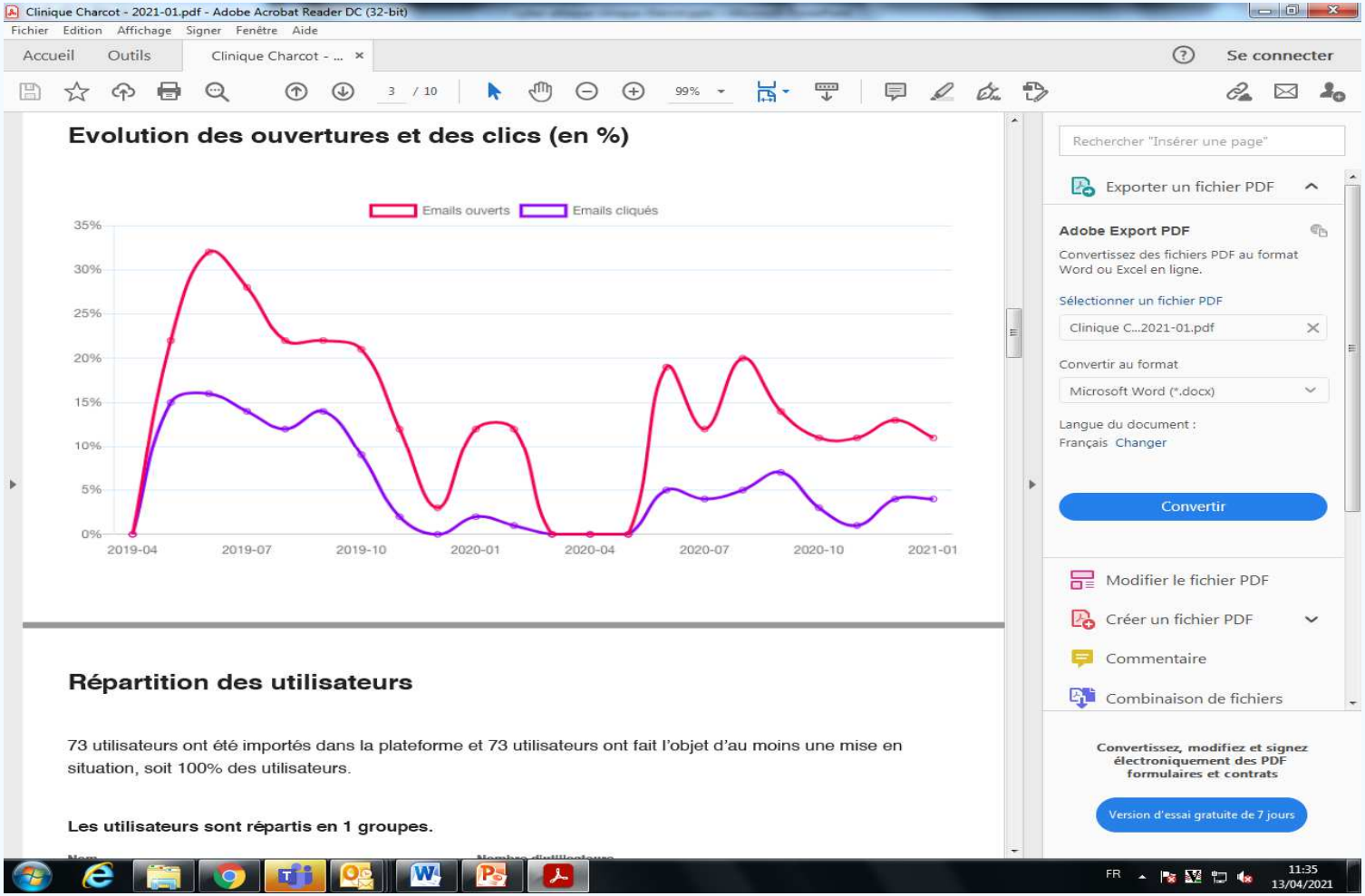
ET la clinique Charcot Sainte-Foy-lès-Lyon

CONTEXTE

- Clinique déjà ciblée par une cyberattaque en février 2016
- DPO motivé sur sa mission
- Un comité de sécurité informatique qui se réunit 1 à 2 fois par an sur le sujet de la sécurité informatique avec le directeur (responsable du système d'information), DPO, responsable dossier patient informatisé et la société qui assure la gestion du réseau
- Une formation mise en place de prévention sur les risques de phishing depuis 2 ans qui a sensibilisé une grande partie du personnel et/ou médecin, score d'ouverture en baisse
- Infogérance en place pour supervision de la sécurité et de l'antivirus sur tous les postes et mise à jour hebdomadaire

CONTEXTE : sensibilisation

Campagne de formation et de prévention (courbe d'évolution)



CONTEXTE : sensibilisation

Sensibilisations sur l'instant

Niveau de risque

Pour rappel voici notre référentiel :

- Rouge : plus de 12% (risque extrême)
- Orange : de 9 à 12% (risque très élevé)
- Jaune : de 5 à 9% (risque élevé)
- Vert clair : de 2 à 5% (risque modéré)
- Vert foncé : moins de 2% (risque minoré)

Cliqueurs uniques

40 utilisateurs ont cliqué sur au moins 1 lien, soit 55 % de la population.
57 templates différents ont été utilisés pour couvrir l'ensemble de la population.

Emails

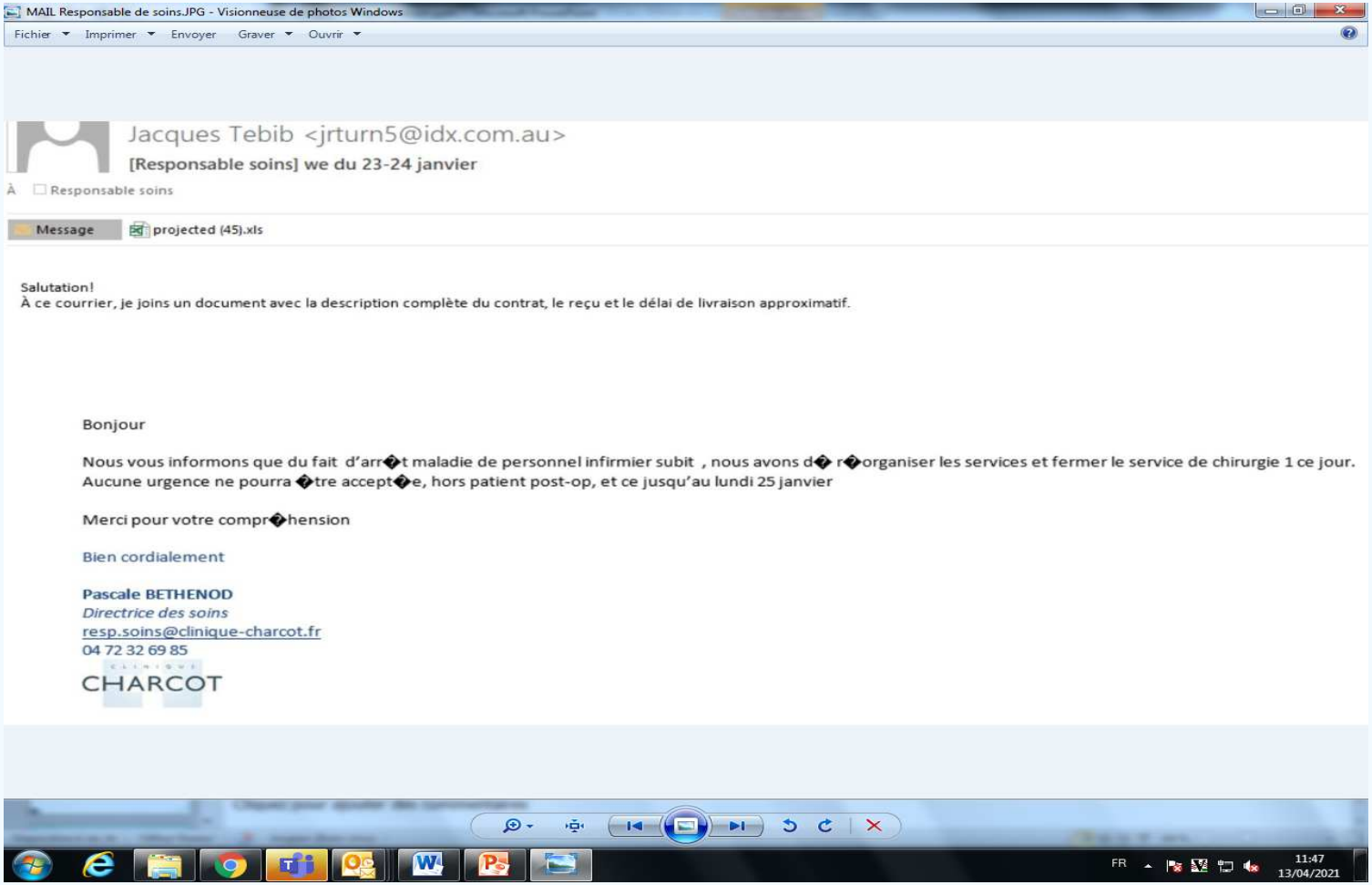
Emails envoyés	1463
Emails ouverts	232 (16 %)
Emails cliqués	90 (6 %)
Probabilité qu'un e-mail ouvert soit cliqué	39 %

Statistiques par template

Nom	E-mails envoyés	E-mails cliqués	Taux d'ouverture	Taux de clic ↓
Candidature suite à l'annonce de la semaine dernière	88	20	32 %	23 %
Exclusivité : parution prochaine d'un article de presse	22	5	32 %	23 %
Quelqu'un a recommandé vos compétences	44	9	27 %	20 %
Palmarès santé : Présence de votre établissement dans le classement trimestriel	78	14	31 %	18 %
Réunion prochaine inter-service	13	2	23 %	15 %
Mise à jour du taux de prélèvement à la source sur les bulletins de salaire	46	6	28 %	13 %
Candidature spontanée	26	3	27 %	12 %
Lancement de votre nouvel Intranet ! Plus intuitif, plus collaboratif et Design !	25	3	28 %	12 %

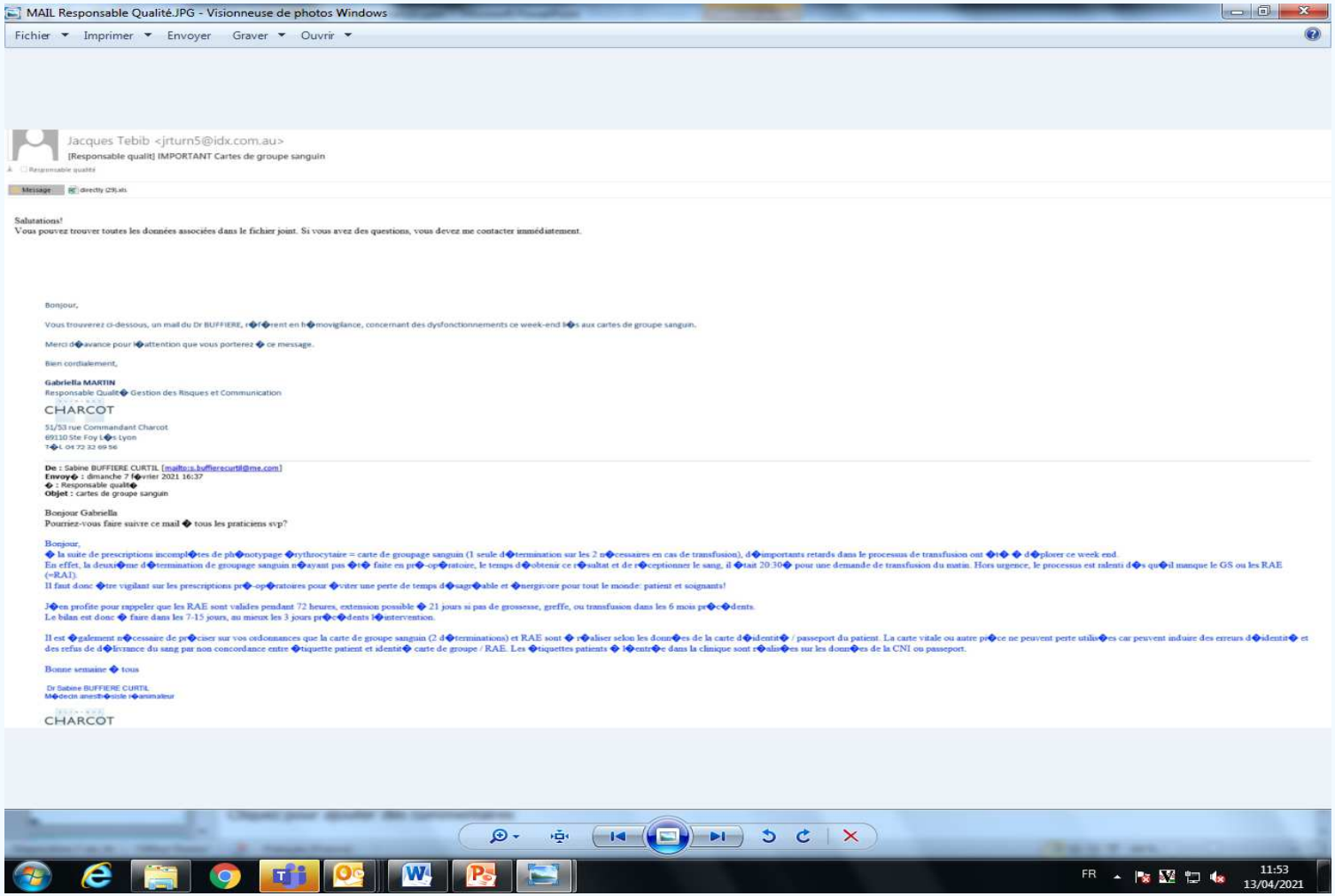
CYBERATTAQUE du 25/02/2021

Description de l'attaque : mail avec PJ



CYBERATTAQUE du 25/02/2021

Description de l'attaque : mail avec virus



CYBERATTAQUE du 25/02/2021

- 20 destinataires différents en interne d'un mail frauduleux avec la même PJ un fichier Excel qui contenait un fichier programmé pour télécharger le logiciel de cryptage en vue d'une demande de rançon
- Surveillance des échanges internes depuis 1 mois, plusieurs mails récupérés émis par différentes personnes via Outlook
- Réponse personnalisée faite à un vrai mail adressé par le destinataire
- Mail adressé par un médecin de la clinique mais avec une fausse adresse dans un laps de temps limité mais pas en série

Mais :

⌧ Réponse sans sens, (robot) sauf celui qui a été ouvert par mégarde
⌧ Adresse mail étrange finissant par .com.au!
⌧ Mail contenant des sigles à la place d'accent, provenance étrangère qui ne connaît pas les accents

CYBERATTAQUE du 25/02/2021

Jacques Tebib <jrturn5@idx.com.au>

[Responsable soins] we du 23-24 janvier

À Responsable soins

Message projected (45).xls

Salutation!
À ce courrier, je joins un document avec la description complète du contrat, le reçu et le délai de livraison approximatif.

Bonjour

Nous vous informons que du fait d'arr�t maladie de personnel infirmier subit , nous avons d� r�organiser les services et fermer le service de chirurgie 1 ce jour.
Aucune urgence ne pourra �tre accept�e, hors patient post-op, et ce jusqu'au lundi 25 janvier

Merci pour votre compr�hension

Bien cordialement

Pascale BETHENOD
Directrice des soins
resp.soins@clinique-charcot.fr
04 72 32 69 85
CLINIQUE CHARCOT

CYBERATTAQUE du 25/02/2021

Détection de l'attaque :

8h30 :

- DPO/RAQ, sensibilisé aux risques informatiques au cours des réunions sur la sécurité informatique, parmi les destinataires, a réalisé immédiatement que la situation était étrange

- Directrice des soins, bureau à coté à celui de la RAQ, également destinatrice du mail infecté mis par ses soins à la corbeille, confirme à la RAQ la réception d'un mail étrange

- Comparaison des deux mails, alerte immédiate de la société informatique qui confirme de n'ouvrir en aucun cas les mails

- Alerte de la Direction

- Lenteur extrême du réseau

CYBERATTAQUE du 25/02/2021

Déroulement des opérations :

8h45 :

- Mail d'alerte adressé immédiatement par la Direction à tous les services de ne pas ouvrir le mail adressé par le soit disant Dr XXX
- Mail doublé d'un contact avec tous les cadres
- Par téléphone, confirmation d'ouverture d'un mail à la direction vers 8h45
- **Application immédiate des consignes prévues à la MARS 10 du 12/2/2021**

En cas d'incident :

 Déconnecter immédiatement la ou les machines concernées du réseau et ne les éteignez pas ;

 Alerter les services informatiques qui mèneront les actions de confinement/investigation/remédiation

Le PC incriminé sur réseau filaire est déconnecté immédiatement du réseau.
Dans le doute sur la situation, même consigne donné pour tous les ordinateurs, tous les membres du service direction sont partis dans tous les services pour s'assurer des arrêts de tous les ordinateurs.

Dans les 10 minutes qui suivent, toute la clinique est à l'arrêt au niveau informatique.

9h00 : le logiciel de cryptage de données et demande de rançon est stoppé dans son téléchargement !

CYBERATTAQUE du 25/02/2021

Mise en place du mode dégradé :

- Édition des plans de suite sur PC de secours
- Documents vierges de traçabilité services/bloc mis à disposition

Au niveau du prestataire :

- Installation du logiciel sur un PC sécurisé sur leur site d'exploitation pour maîtriser les incidences de ce virus
- Envoi de 2 agents pour faire le point sur site
- **Confirmation à 11h00 que grâce aux mesures prises, les serveurs de base de données ne sont pas touchés**
- **Définition des critères de priorisation dans l'audit sécuritaire de chaque ordinateur avant remise en service**

CYBERATTAQUE du 25/02/2021

Alertes auprès des tutelles :

- **Notification faite à l'ARS** par téléphone dès que le bilan de la situation a pu être fait, puis par mail à l'adresse de crise

- **Déclaration faite de l'incident** sur le portail dédié à cet effet, conformément à l'article L.1111-8-2 du code de la santé publique https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil)

- **Dépôt de plainte fait** auprès des services de police ou de gendarmerie dont vous dépendez, ou auprès du procureur de la République du tribunal judiciaire dont vous dépendez

- **Pas de déclaration à la CNIL** via le lien https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles car pas de violation de données à caractère personnel

CYBERATTAQUE du 25/02/2021

Analyse post mortem : les points positifs

- La réactivité des équipes et un peu de chance ont permis de bloquer à temps le téléchargement du logiciel de cryptage et de demande de rançons
- Une prise de conscience immédiate par l'ensemble de la clinique de la gravité de la situation et une participation active au mode dégradé
- La connaissance des consignes de déconnecter tout ordinateur, application de la MARS dernièrement reçue
- Continuité des soins assurée grâce aux plans de soins qui a pu être édité sur PC de secours
- Programme opératoire qui a pu être maintenu grâce à une IDE qui l'édite tous les jours sur support papier!
- Les supports d'envoi de SMS faits la veille pour fixer les horaires qui ont permis de connaître les entrées de J+1
- Les documents vierges de toute traçabilité qui étaient conservés

CYBERATTAQUE du 25/02/2021

Analyse post mortem : les points négatifs

- Simulation cyberattaque testée en direct
- Oubli du réseau WIFI et déconnexion des PC mobiles dans un deuxième temps (mais non destinataire de messagerie)
- Méconnaissance de comment couper le réseau WIFI
- Certains PC ont été oubliés
- Protocoles médicamenteux non disponibles (les ordinateurs étant coupés plus d'accès aux protocoles dans logiciel démarche qualité)
- Listes des téléphones et astreintes non disponibles pour les mêmes raisons
- Documents de traçabilité papier non maîtrisés par les nouveaux embauchés (il a fallu faire une mini-formation par les anciens sur les courbes de température...)
- Certains services avaient jetés ces documents de traçabilité papier car ne servant plus à rien !

- Mais pas de visibilité sur les entrées à J+2

CYBERATTAQUE du 25/02/2021

Analyse post mortem : les enseignements

- Coordonner la reprise des prescriptions bloc/services lors de la remise en service des PC

- Réflexion sur mise en place d'un classeur de secours avec les infos tels astreintes, protocoles médicamenteux… : qui le tient à jour ? Sous quel format ?

- Mise en place de disjoncteurs en salle informatique pour isoler les serveurs beaucoup plus rapidement et de manière plus sécurisée (plus d'oubli de PC à débrancher)

- Procédure de sauvegarde à élargir sur les logiciels périphériques

Conclusion : toujours rester vigilant malgré tous les efforts apportés à la sécurité ; « 100 % des attaques qui aboutissent sont dues à une intervention humaine », dixit la police judicaire. Attention dans le futur à l'intelligence artificielle qui peut devenir capable de structurer ses

CYBERATTAQUE du 25/02/2021

Les actions d'améliorations menées :

- Réseau téléphonique isolé
- Sauvegardes doublées et externalisées pour minimiser l'impact à 48h d'indisponibilité
- Centralisation coupure des ordinateurs en isolant le local serveurs
- Rajout sur le PC de secours des documents en sus des plans de soins type, entrées à venir, programme du bloc opératoire

CYBERATTAQUE du 25/02/2021

Que s'est-il passé après ?

Eléments d'informations fournis à La Cellule ACSS cyberveille@esante.gouv.fr pour enquête internationale

CYBERATTAQUE du 25/02/2021

Bilan : à quoi a t'on échappé ?

- Plus de dossiers médicaux : avec des patients en maladie chronique
- Perte de toutes les données : entrées futures des patients inconnues
- Perte des données financières : facturation bloquée, suivi des règlements impossible, factures des fournisseurs perdues, règlement des fournisseurs impossible, dépôt de bilan ????
- Attaque la veille du virement des paies ! : plus de données pour les virements
- Diffusion de données sur Internet : infraction avec la loi RGPD, problématique avec la CNIL
- La solution : payer la rançon ? rien ne garantit la récupération des données avec le risque de payer plusieurs fois

Centre Hospitalier Albertville - Moûtiers

RETEX cyberattaque fin décembre 2020

Sonia Rasle - DSIO CH Métropole Savoie / DSI du GHT Savoie-Belley

Contexte avant l'attaque

Contexte national

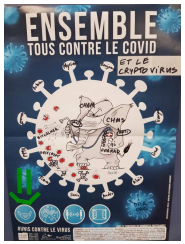
- Fin 2ème vague Covid
- Période de fin d'année
- Début vaccination Covid
- Appui national limité

Contexte local

- Covid Savoie département le plus touché fin 2020 (taux incidence 1.200)
- Absence Directeurs CHAM + CHMS au début de la crise (congés)
- Top management nouvellement arrivés
- Neige++
- Stations de ski fermées

Contexte CHAM

- CHAM : 450 lits, 1.100 agents
- Fatigue liée à l'année Covid
- Arrivée du RSSI du GHT fin 2019
- Formations de sensibilisation sécurité SI annulées cause Covid vagues 1 et 2



Contexte SI

Pb de gouvernance SI
- RSI poste vacant depuis 6 mois
- Equipe en difficulté
- Pas de gestion de parc
- Absence de politique de mdp
- Comptes AD en surnombre
- Moûtiers pas de svgde sur bandes
- Référents métiers non identifiés

- SI crypté dont doc SI
- Perte des moyens de communication
- Pas de visi sur la programmation (consult, hospit, bloc...)
- Pas de liste de personnels
- Moûtiers perte de données
- Gouvernance SI à revoir

Centre Hospitalier Albertville-Moûtiers

Description de la cyberattaque

CENTRE HOSPITALIER MÉTROPOLE SAVOIE

- **08/12/2020 - 1ère attaque : virus cryptominer**

  qui permet la fabrication de cryptomonnaie

  => saturation des serveurs

  Virus éradiqué mais vulnérabilité du SI non détectée

- **Dimanche 20 au 21/12/2020 (entre 22h30 et 3h) - 2ème attaque : cryptovirus**

  Intrusion initiale via une vulnérabilité dans le pare feu (appareil de protection du réseau qui surveille le trafic entrant / sortant de l'hôpital)

  Permet à des attaquants non authentifiés d'accéder à des informations sensibles (comptes et mots de passe des utilisateurs)

  => chiffrage toutes les données du SI

  => demande de rançon

Détection de l’attaque par le CHAM le 21/12

- **Evaluation instantanée** par l'informaticien d'astreinte appelé à 4h du matin = **problème de grande ampleur** : demande de rançon + serveurs inaccessibles + PCs cryptés

- **Déclaration dans la nuit de l'incident** sur le site national DGOS des événements indésirables, rubrique SI

- **Appel à l'aide** de l'établissement support du GHT = CH Métropole Savoie (CHMS à Chambéry)

Mobilisation & cellule de crise

- **Mobilisation** par l'établissement support CHMS **de la 1ère cellule de crise du CHAM à 9h30**

- **Composition** : représentants médicaux de la CME, du DIM, du service informatique, de la Direction du CHAM, du RSSI de GHT, du DSIO du CHMS et de la Direction générale du CHMS

- **Fréquence des cellules de crise**

Impacts sur le SI

Etat des lieux débuté le 21/12 ... long à établir (plus de cartographie)

- SI hors service - sauf téléphonie et biomédical
- Données des serveurs Windows et une partie des PCs du CHAM chiffrées donc inaccessibles
- Pas d'exfiltration de données
- Pas ou peu d'impact sur les patients hospitalisés lors de la cyberattaque et pour les prises en charge qui ont suivi
- Données hébergées sur le site de Moûtiers définitivement perdues :
  - Ancien DPI : historiques prescriptions, pancartes, actes CCAM, CR bio, antériorités bloc, rétrocessions médicaments, DMI, historique MDS
  - PMSI, régul activité 2019 (lambda)
  - GED (GDR, FEI)
  - Images échographies

Centre Hospitalier Albertville-Moûtiers

Plan d'actions

CENTRE HOSPITALIER MÉTROPOLE SAVOIE

- **Phase 0 - Mesures conservatoires**
  - Temps de la sidération, mesures immédiates, alerte aux établs du GHT et fournisseurs d'hébergement, orga cellule de crise et suivi (CR et main courante), déclarations d'incident (ACSS, CERT-FR, ANSSI) et de violation de données (CNIL), dépôt de plainte (PJ), communication interne et communiqués de presse externes, mobilisation moyens internes et externes
  - Confinement et figeage du SI (protéger les sauvegardes, couper internet, conserver les systèmes contaminés)

- **Phase 1 - Restitution**
  - Analyser l'attaque, état des lieux, décontaminer, qualifier les fonctionnements dégradés, restituer les principales fonctions du SI sur une architecture provisoire

Plan d'actions

- **Phase 2 - Remédiation**
  - Correction des failles de sécurité exploitées et amélioration des pratiques
  - Appui société spécialisée en cybersécurité
  - Etape préalable à la réouverture d'internet
  - Mise à niveau des PCs et serveurs, nettoyage des comptes admin et utilisateurs, politique mot de passe révisée et changement de tous les mots de passe, tests d'intrusion externes
  - Réouverture Internet = SORTIE DE CRISE pour les utilisateurs « lambda »

- **Phase 3 - Gouvernance et architecture cible**
  - Gouvernance SI renforcée et mutualisé GHT, architecture cible conforme ANSSI en 3 tiers, plan de formation de l'équipe SI, PSSI GHT, démarche de sensibilisation des utilisateurs à la sécurité numérique

Temps de retour à la normale + coûts

- **Temps de retour à la normale**
  - Quelques applis accessibles le 31/12 à J11 sur des PCs isolés avec clés 4G
  - GAM remontée à J15
  - Paie + messagerie interne à J17
  - DPI à J26 avec démarrage progressif pour reprise des données papiers/informatiques faits depuis le début de l'attaque
  - Internet + messagerie vers extérieur rouvert à J85
  - 1 an après... reste encore HS la QGDR et gestion archives papiers

- **Impact financier**
  - Estimé à 1,5 M€

Enseignements à retirer

- **DSIO**
  - **Sauvegardes sur bandes** - à isoler, cartographie à mettre à jour, cloisonner les réseaux, rétentions de logs (pare feu, Windows) sur 6 mois mini, minimiser et ségréger les comptes des administrateurs (règle du moindre privilège et périmètre - comptes individuels - double authentification pour accès distants), adapter la politique de mots de passe
  - **Absence d'intervention** des experts ANSSI et du ministère sur site, manque de coordination-échange entre ACSS et ANSSI
  - Faire appel sans délai à un **prestataire de réponse aux incidents** de sécurité (PRIS)
  - 6 mois de vacance du poste RSI = équipe SI pas organisée, donc panique
  - **Forte mobilisation** immédiate GHT : DSIO GHT, RSSI GHT et ingénieurs CHMS
  - **Mobilisation rapide** de quelques fournisseurs **(Hopsis, Sara) ou confrères (HCL)**

Enseignements à retirer

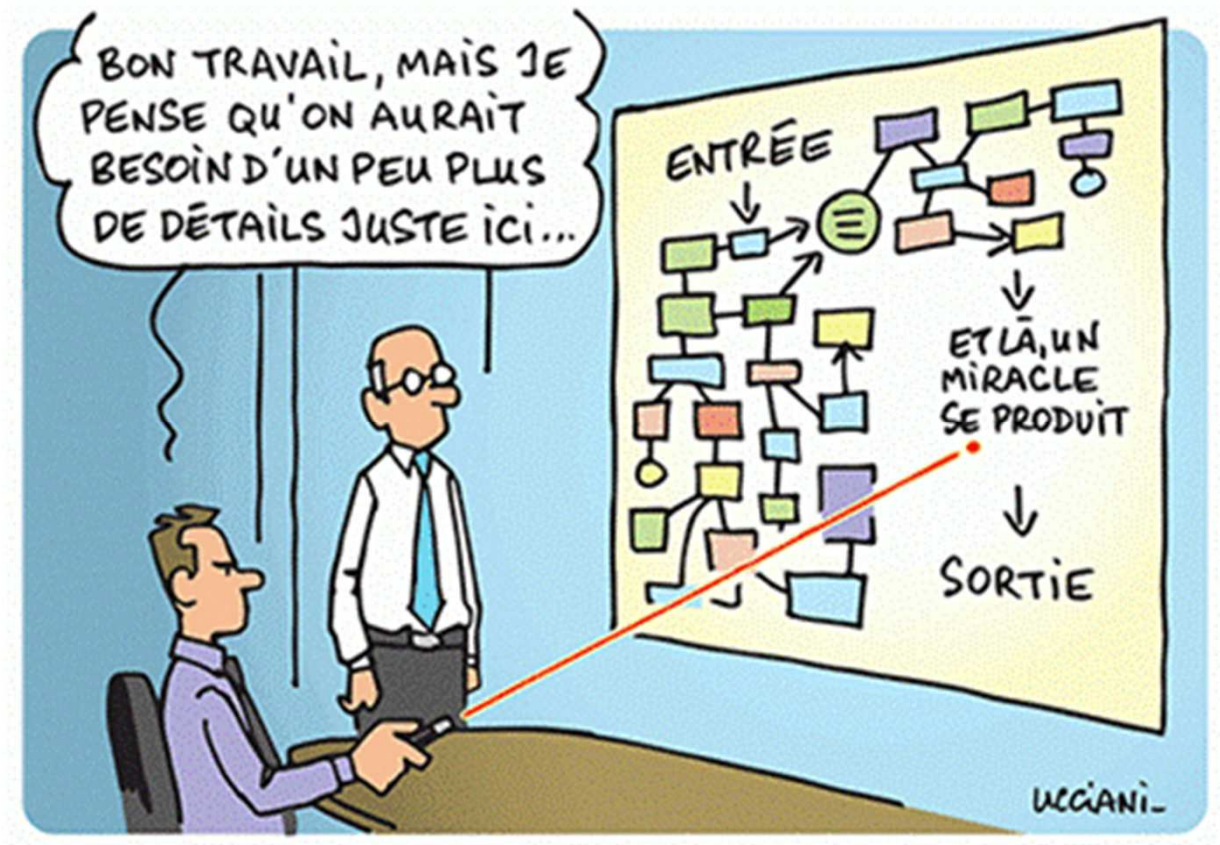
- **Organisation**
  - Se préparer à la gestion de la crise
  - Avoir des procédures de pannes connues
  - Être agile et s'adapter en permanence (la cellule de crise décide des priorités et arbitrages)
  - Résilience ++ des personnels, calme et solidarité
  - Chance d'avoir gardé des anciens supports papiers « oubliés dans un coin »

- **Recommandations**
  - Ne pas négliger les aspects psycho : épuisement équipe SI à J3, cauchemars affreux, droit de retrait des soignants/médecins, 1 an après traumatisme encore présent chez certains
  - Mettre des moyens en € (5% mini du budget SI) et en RH (ETP et compétences à mutualiser)

Centre Hospitalier Albertville-Moûtiers

Des questions ?

CENTRE HOSPITALIER MÉTROPOLE SAVOIE



RETEX cyberattaque du 15 février 2021
GHT Rhône Nord Beaujolais Dombes

Olivia DECLERCK - Médecin Urgentiste
Nasser AMANI - Directeur des Services Numériques du Territoire

GHT RHÔNE NORD BEAUJOLAIS DOMBES

337 000 habitants

2 départements

9
Etablissements MCO/ SSR

14
EHPAD

5
Partenaires

435,6M€
Budget total

3138
Lits

200 726
Consultations

86 682
Passage aux urgences

443
Médecins

4247
Personnels

Chronologie de la Cyberattaque

l'hôpital NORD OUEST

Cyber Attaque Phase de Chiffrement
15 fév.

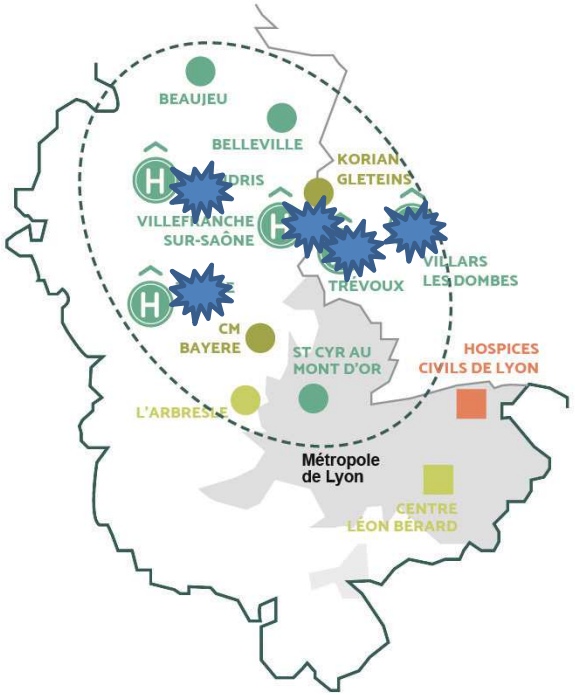
Conf Call PR
Visite O. VERAN – C. O

Aujourd'hui

	Février 2021	Mars 2021	Avril 2021	Mai 2021	2022
Incident	**Identification - Confinement** ● ⇨ Arrêt du Système d'Information ⇨ Passage en mode dégradé ⇨ Analyse impacts sur notre SI (Pas de perte de données, sauvegardes non touches, pas d'extraction de données) ● Déclaration de l'incident de Sécurité (ANSSI, CNIL, ANS…)				

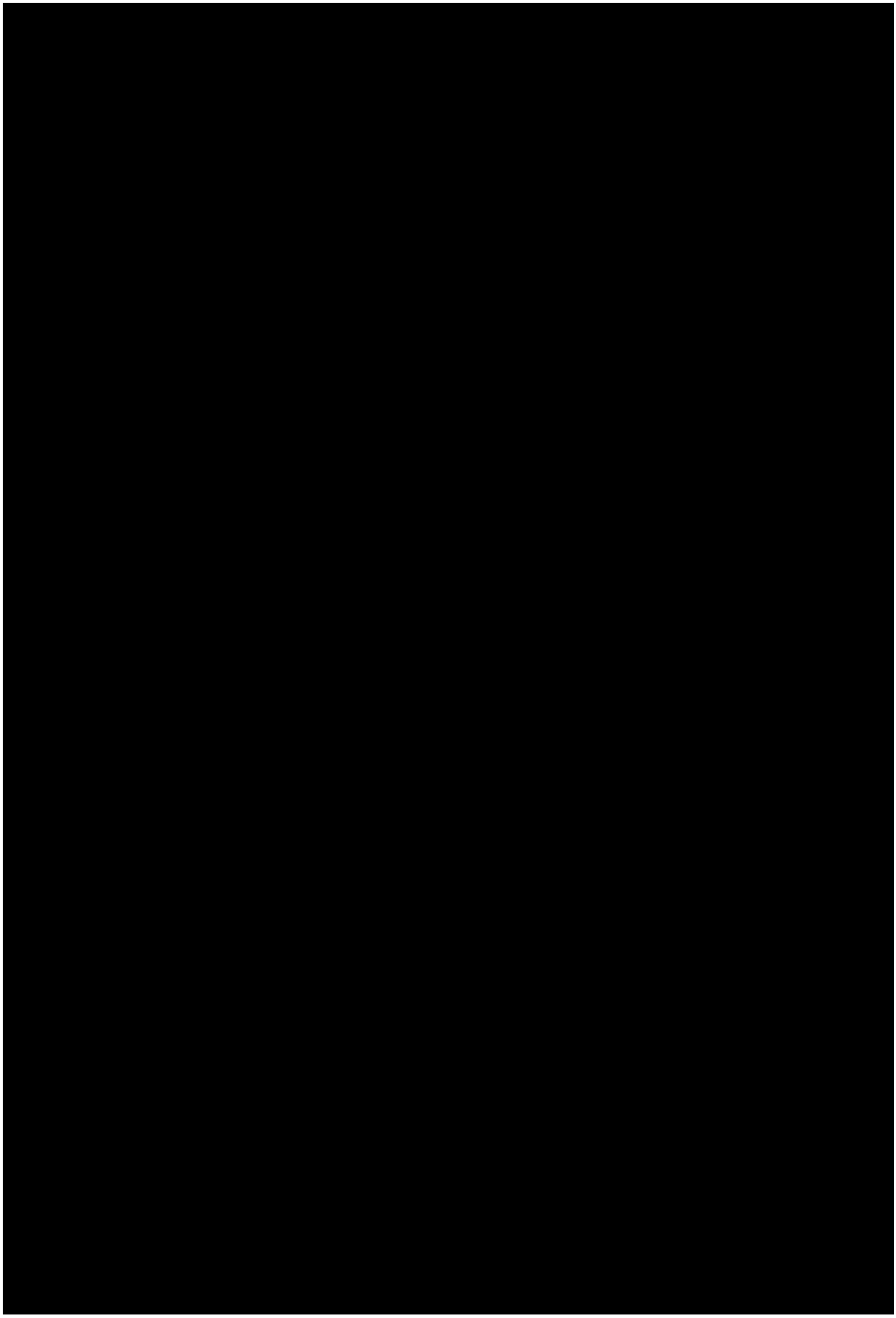
J0 : Le jour de l'attaque

Lundi 15 février 2021



- **Contexte :**
  - 2ème semaine vacances scolaires
  - Nuit profonde
  - Sortie de 2ème vague Covid
- **Dans les faits :**
  - 04h45: aucun logiciel ne fonctionne
  - 05h00: Alerte Cyberattaque
- **Consigne:**

Eteindre tout le système informatique !!!



Plus d'accès à :

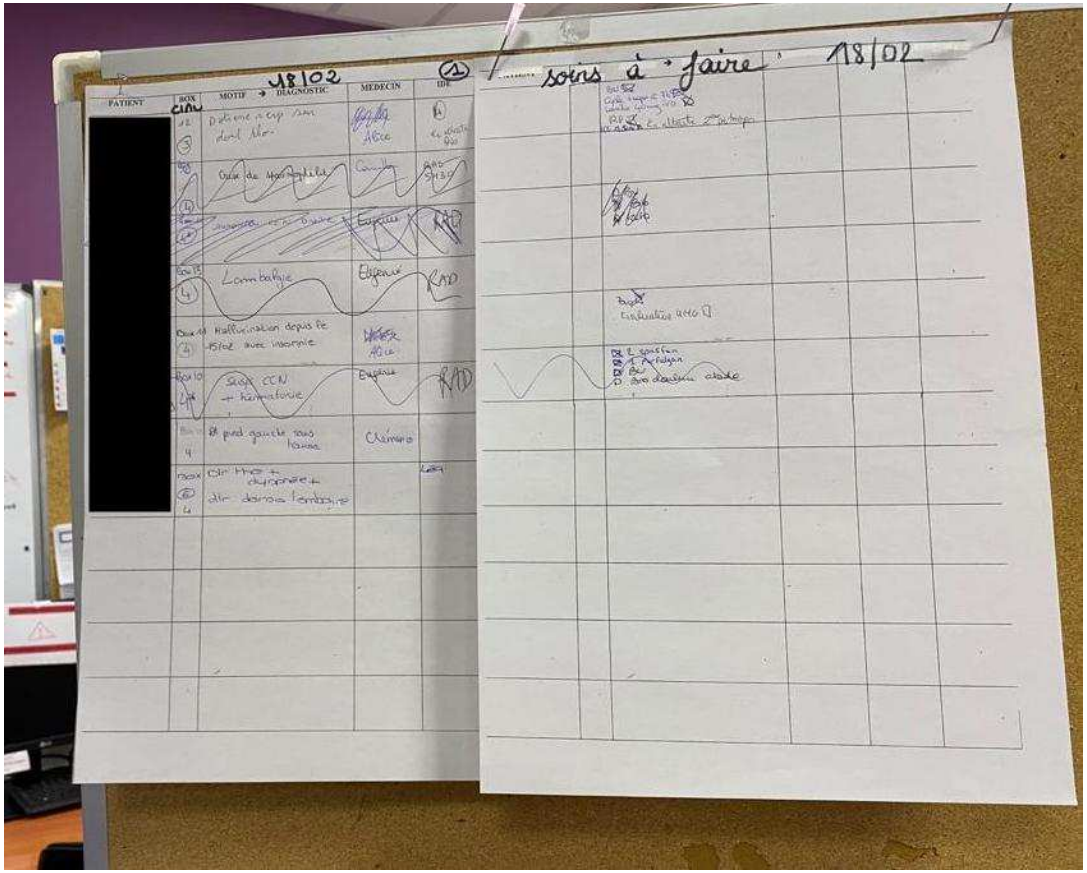
- Dossier médical
- Prescriptions
- Imagerie, laboratoire
- Surveillance par scope
- Informations administratives
- Logistique: caméra, climatisation …
- Téléphonie interne et externe

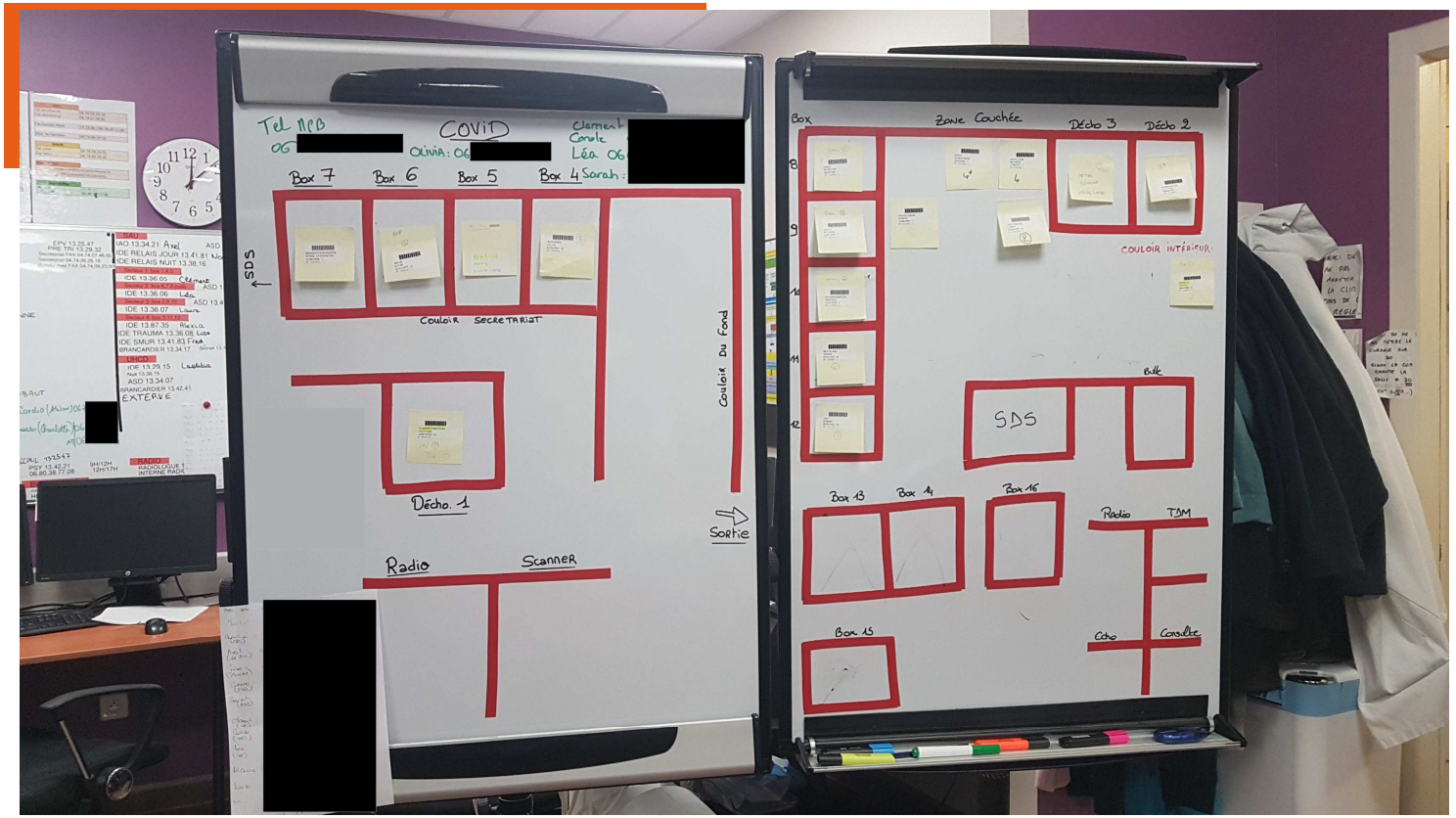
Gestion de la crise: les premiers réflexes

- **Alerter:**
  - Les autorités : ARS, ANSSI
  - Les régulations SAMU pour détourner les flux (baisse de 35 à 50% d'activité aux Urgences)

- Récupérer les données sauvegardées sur les ordinateurs « mode dégradé » de chaque service

Lister et localiser les patients




Tel NCB
COVID
Box 7
Box 6
Box 5
Box 4
SDS
Couloir Secretariat
Couloir Du Fond
Déco. 1
Sortie
Radio
Scanner
Box
Zone Couchée
Déco 3
Déco 2
COULOIR INTÉRIEUR
SDS
Box 13
Box 14
Box 16
Radio
TDM
Box 15
Déco
Couloir

Chronologie de la Cyberattaque

l'hôpital NORD OUEST

Cyber Attaque Phase de Chiffrement
15 fév.

Conf Call PR
Visite O. VERAN – C. O

Aujourd'hui

	Février 2021	Mars 2021	Avril 2021	Mai 2021	2022
Incident	**Identification - Confinement** ⇨ Arrêt du Système d'Information ⇨ Passage en mode dégradé ⇨ Analyse impacts sur notre SI (Pas de perte de données, sauvegardes non touches, pas d'extraction de données) Déclaration de l'incident de Sécurité (ANSSI, CNIL, ANS…)				
Gestion de la crise - Gouvernance	**Pilotage de la Cellule de crise** ⇨ Plan de continuité d'activité ⇨ Plan de reprise d'activité et de retour à la normale ⇨ Lien avec Présidence, ARS, Ministères, Enquête ⇨ Lien avec la presse et les medias			**Etes vous prêt ?**	

Chronologie de la Cyberattaque

l'hôpital NORD OUEST

Cyber Attaque Phase de Chiffrement
15 fév.

Conf Call PR
Visite O. VERAN – C. O

Aujourd'hui

Février 2021 | **Mars 2021** | **Avril 2021** | **Mai 2021** | **2022**

Incident

Identification - Confinement

- ⇨ Arrêt du Système d'Information
- ⇨ Passage en mode dégradé
- ⇨ Analyse impacts sur notre SI (Pas de perte de données, sauvegardes non touches, pas d'extraction de données)

- Déclaration de l'incident de Sécurité (ANSSI, CNIL, ANS…)

Gestion de la crise - Gouvernance

Pilotage de la Cellule de crise

- ⇨ Plan de continuité d'activité
- ⇨ Plan de reprise d'activité et de retour à la normale
- ⇨ Lien avec Présidence, ARS, Ministères, Enquête
- ⇨ Lien avec la presse et les medias

Etes vous prêt ?

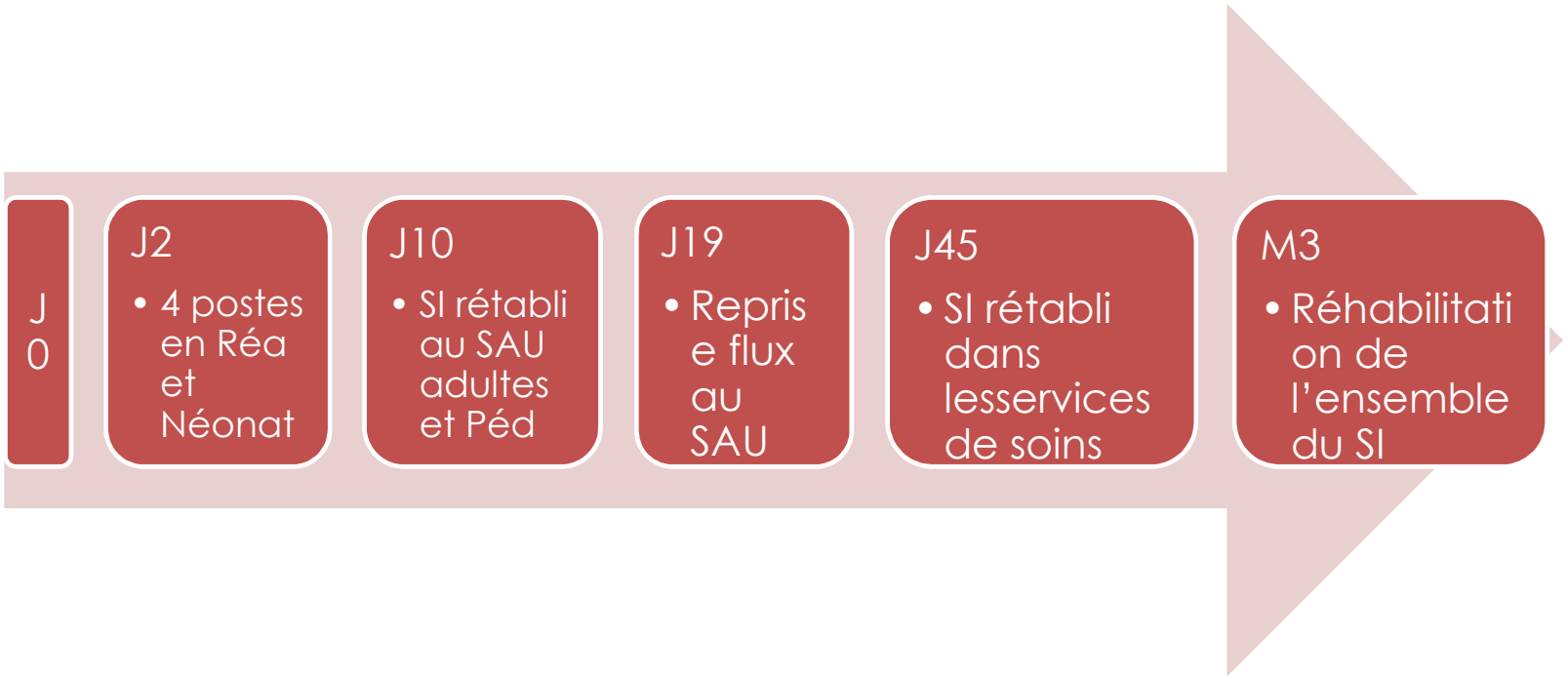
Remédiation

- **Phase de Reconstruction du SI : Eradication - Récupération**
  - ⇨ Définition de la stratégie de remédiation
    - ⇨ Nuit du 17 au 18/02/21 : Remise en marche de poste en réanimation et en Néonatologie
    - ⇨ 25 février : Relance du SI des Urgences
      - ⇨ Relance progressive et séquencée de tous les services et établissements

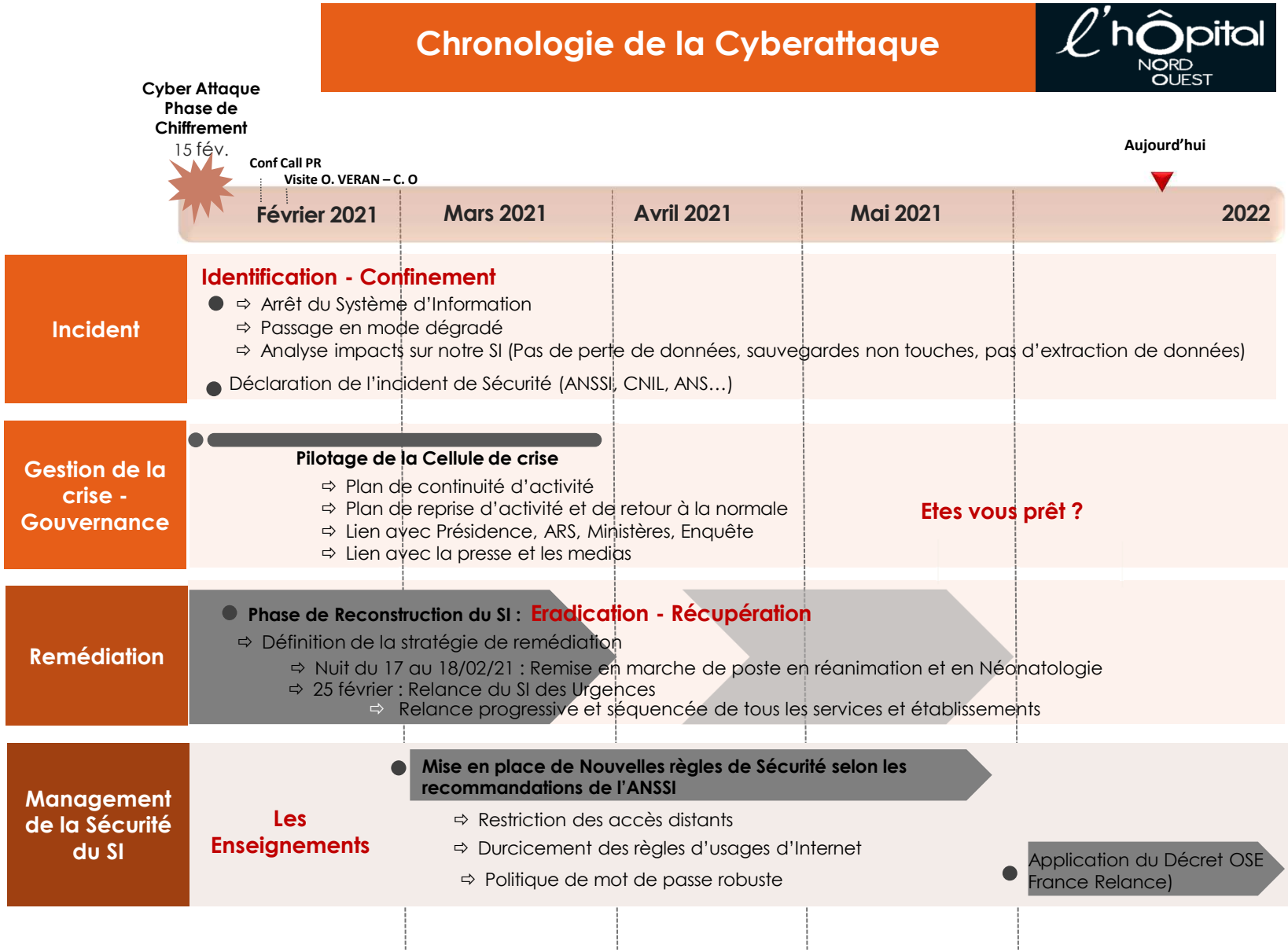
Gestion de la crise...dans la durée

- Procédures « papier-crayon »
- Etiquettes manuscrites et identito-vigilance
- Biologie et Imagerie en dégradé : allongement des délais et saturation des capacités
- Bloc opératoire: à minima
- Pas d'admission en réanimation: transfert des patients instables

Remédiation du système d'information



Chronologie de la Cyberattaque



Les pistes d'amélioration pour les soignants

- Comité RETEX et réécriture des procédures dégradées
- Formation du personnel aux procédures et exercices Cyber
- Anticipation d'une panne plus étendue et plus durable
- Recherche d'une alternative à la téléphonie interne
- Education à l'hygiène numérique

Aucun établissement n'est à l'abri ! Cela n'arrive pas qu'aux autres !

- Protéger : Confiner le SI - Débrancher immédiatement les câbles réseau.
- Alerter : Détourner rapidement le flux de patients.
- Sauvegarder : Récupérer les sauvegardes de prescriptions.

Intégrer le risque CYBER dans nos procédures Plan blanc

- Prévoir en amont tous les documents sur papier.
- Faire connaître la procédure dégradée.
- Avoir un ordinateur + imprimante hors réseau (étiquettes de patient).

→ Réaliser des exercices Cyber et tester les équipes

Notre force aujourd'hui est de savoir que cela peut nous arriver à nouveau !

Questions / Réponses

Conclusion

RANÇONGICIEL Vos données sont prises en otage

REACTION

COMMENT RÉAGIR ?
Vous êtes victime d'un rançongiciel
Ne payez pas !

1 - Ne pas éteindre la machine concernée
La mettre en veille prolongée si possible

2 - Déconnectez immédiatement les appareils du réseau

3 - Ne connectez plus aucun appareil sur le réseau

4 - Contactez immédiatement votre service informatique ou un expert (ou trouvez le vôtre sur www.cybermalveillance.gouv.fr)

5 - Portez plainte auprès des services compétents

QUE SE PASSE-T-IL ?

1. Vos données sont progressivement chiffrées, ce qui les rend inaccessibles

2. L'infection peut s'étendre à tous les appareils connectés au réseau ou aux supports USB branchés

3. On exige de vous le paiement d'une rançon pour récupérer ces données

Impact de l'attaque
Intégrité
Disponibilité
Confidentialité
Authenticité

Motivations principales
Atteinte à l'image
Appât du gain
Revendication
Espionnage
Nuisance

PROTECTION

COMMENT SE PROTÉGER ?
Ne tombez pas dans le piège

Effectuez des sauvegardes régulières de vos données

Mettez à jour régulièrement vos principaux logiciels
- Les rançongiciels utilisent les vulnérabilités des programmes pour se propager

Privilégiez un compte utilisateur pour vos usages courants

Courriers électroniques piégés
- Ne faites pas confiance à l'expéditeur de courriers électroniques dont l'origine ou la forme vous semblent douteuses
- Méfiez-vous des pièces jointes et des liens suspects

En savoir plus sur les attaques par rançongiciel :
www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/
www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Des actions pragmatiques d'appui de l'ARS et du GCS SARA aux ES

1. Sensibiliser les acteurs en établissements

- ✓ A travers des **webinaires**
  - ✓ à destination des ESMS (ARS/Grades/Gendarmerie nationale) : 2 en 2021-22
  - ✓ À destination des établissements sanitaires : ex. ce jour
- ✓ Atelier **d'expression des besoins** ES (nov. 2021)
- ✓ Accord et personnalisation d'un *escape game*

2. Fédérer la chaîne des acteurs ES-Grades-ARS

- ✓ Créer et co-animer un **collège régional** RSSI
- ✓ Proposer et mettre en œuvre un **portail régional collaboratif** : partage documentaire, kits mise en œuvre PCA, outils de management de la sécurité, tutoriels
- ✓ **Recrutement** d'une ressource dédiée à la coordination : Référent sécurité Grades,
- ✓ Identifier des **relais en établissements** : pairs, ambassadeurs, …

Des actions pragmatiques d'appui de l'ARS et du GCS SARA

3. Identifier ensemble les actions concrètes et réalistes pour

- ✓ Référencer des **outils** avec RETEX (*benchmark*)
- ✓ Référencer des **offres de formation**
- ✓ Mettre à disposition des **outils pédagogiques** : escape game, e-learning, tutos, …
- ✓ Définir un **plan de déploiement** de ces mesures (20ES→50 ES →100 ES, …)

4. Impliquer les ESMS qui développent leur SI (Ségur, TLM) dans la démarche

QU'EN PENSEZ VOUS ?

Merci de votre participation !