LECTURE
du guide d'aide à la préparation
Plan blanc numérique

Juin 2023

Mission SSE/NRBC – ESR Rouen
Zone de défense et de Sécurité Ouest

3 parties avec plusieurs chapitres

- Prévenir le risque numérique
  - Maitriser ses systèmes d'information
  - Formaliser un plan de mise en conformité adapté
- Elaborer le volet numérique
  - Les modalités de mise en œuvre
  - Les éléments généraux à préparer
  - Se préparer aux étapes à suivre
- L'organisation des soins
  - L'impact sur l'organisation des soins
  - La prise en charge en mode dégradé

Elaboration du VOLET NUMERIQUE du Plan blanc

PARTIE 1 : Prévenir le risque numérique

Chapitre 1 : Maitriser ses systèmes d'information

- Disposer de ressources humaines pour sécuriser le système d'information

- L'importance des cartographies du système d'information

- L 'analyse du risque

1.1 Désignation d'un responsable de la sécurité des systèmes d'information = RSSI

- Il est désigné par le Directeur de l'ES et devient l'interlocuteur des professionnels
- Le RSSI est chargé
  - De promouvoir et accompagne les bons usages quotidiens et les pratiques de sécurisation au quotidien
  - De sensibiliser l'ensemble des acteurs à la prévention du risque numériques
  - De définir des actions de sécurisation
  - D'organiser des diagnostics, des analyses de postes, des audits
  - De mener des actions de sensibilisation et d'information par des simulation, des actions de formation
  - De rendre compte semestriellement à la gouvernance de l'évolution des risques

1.2 Des ressources techniques adaptées au maintien en sécurité

- Il est nécessaire d'adapter l'effectif des ressources techniques au regard des taches à accomplir

1.3 L'implication du service en charge des systèmes d'information

- Il est nécessaire d'intégrer la cybersécurité lors des étapes de procédure de passation de marché, notamment en outils de télémaintenance

1.4 La sensibilisation du personnel

- Le personnel doit être informé des menaces.
- Une action de sensibilisation à la sécurisation doit être inscrite au plan de formation annuel
- Cette thématique doit être abordée lors des journées d'accueil des nouveaux arrivants
- Un affichage permanent des principales recommandations doit être lisible dans les services

PARTIE 1 : Prévenir le risque numérique

Chapitre 1 : Maitriser ses systèmes d'information

- Disposer de ressources humaines pour sécuriser le système d'information
- L'importance des cartographies du système d'information
- L 'analyse du risque

2.1 La nécessité de réaliser une cartographie précise

- Document fiable et à jour
- Document complet des ressources informatiques avec les connexion internes et externes
- Outil indispensable au pilotage de l'évolution du système

2.2 Le contenu de la cartographie

- Tous les éléments fonctionnel prioritaires
- Ensemble des actifs matériels, logiciels métiers et de services, les connexion réseau
- Les prestataires et partenaires extérieurs

Pour aller plus loin, le guide « Cartographie du système d'information, guide d'élaboration en cinq étapes » publié par l'ANSSI présente une démarche adaptée aux besoins opérationnels des organisations et propose une approche pratique et progressive pour avancer pas à pas dans l'élaboration d'une cartographie.

Document socle lors d'un évènement numérique

PARTIE 1 : Prévenir le risque numérique

Chapitre 1 : Maitriser ses systèmes d'information

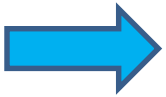
- Disposer de ressources humaines pour sécuriser le système d'information
- L'importance des cartographies du système d'information
- L 'analyse du risque

3.1 Les typologies de menaces

- Une analyse approfondie des risques est fondamentale pour identifier les menaces de l'ES
- Classification nécessaire :
  - Acte malveillant
  - Sinistre
  - Perte de services essentiels
  - Compromission des données
  - Défaillance technique

3.2 L'importance d'identifier les applications métiers critiques

- Nécessité d'évaluer la criticité sur une échelle de 1 à 4 de l'interruption en fonction
- Nécessité de connaitre les impacts sur les applications métiers
- En amont, identifier les systèmes clés qui permettent la continuité des soins



Un facteur de criticité et une durée maximale admissible d'indisponibilité doit être associée à chaque composant du système

3.3 Le repérage des applications métiers hors schéma directeur

- Nécessité de repérer les applications qui ne sont pas répertoriés au sein de l'inventaire direction

3.4 L'identification des vulnérabilités

- Identifier les actifs potentiellement impactés et préciser les points de fragilité
- Evaluer l'impact du risque sur des différentes composantes :
  - Production de soins
  - Administratif
  - Logistique
  - Volet légal et réglementaire
  - Recherche
  - Image

3.5 Des structures de soins qui partagent des données sensibles

- La mise en œuvre de contre mesures doit être prévue
- Nécessité de travailler sur les protocoles et conduites à tenir en cas d'évènement numérique

3.6 La prise en compte des liaisons internes

- Nécessité dans l'analyse des risques de prendre en compte tous les partenaires extérieurs
- L'intrusion peut être faite suite à une défaillance chez un partenaire extérieur

3.7 Attention particulière à la télémaintenance

- Attention lors d'utilisation de réseau public
- Consulter note technique « recommandation de sécurité relatives à la téléassistance » de l'ANSSI

3.8 Les risques liés aux dispositifs médicaux connectés

- De plus en plus nombreux au sein des structures hospitalières

3.9 La gestion des centrales de surveillance

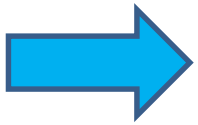
- Vigilance aux services de réanimations et de haute technicité qui utilisent ces centrales pour veiller sur les patients

3.10 Les outils de collaboration cliniques inter-établissements

- Une évaluation des ces outils semblent nécessaires dans le cadre de leur acquisition

3.11 Evaluer la vulnérabilité de l'annuaire central

- Clé de voute du système d'information d'un ES
- Permet aux administrateurs de
  - Gérer les droits d'accès
  - Authentifier les connexions
  - Déterminer les ressources auxquelles y accèdent
- Nécessité d'une politique de sauvegarde spécifique



CIBLE de choix pour les attaquants

Fiche réflexe 1 : maîtriser son système d'information

- Désigner un responsable de la sécurité des systèmes d'information

  - Évaluer la possibilité de mutualiser son intervention au sein du GHT
  - Interlocuteur privilégié sur le périmètre de la cybersécurité

- Impliquer le département informatique dans les processus d'acquisition

  - Acquisition des dispositifs médicaux connectés
  - Application des principes du « *privacy by design* » dans la gestion de projet

- Sensibiliser le personnel

  - Organiser une action de sensibilisation dans le programme de formation
  - Organiser des exercices et simulation de problèmes informatiques

- Réaliser et tenir à jour des cartographies du système d'information

  - Repérer les matériels, logiciels, connexions réseaux
  - Evaluer et repérer la criticité des systèmes d'information
  - Repérer les serveurs stockant des données sensibles
  - Repérer les composants du système d'information hors schéma directeur
  - Définir l'ordre de priorité de remise en service des applications métiers
  - Repérer les connexions avec les systèmes d'information externes
  - Repérer les opérateurs de télémaintenance
  - Limiter les accès à la cartographie du système d'information, confidentialité
  - Mettre à jour régulièrement la cartographie

- Effectuer une analyse des risques du système d'information

  - Identifier les menaces potentielles et leurs impacts
  - Évaluer les vulnérabilités des applications métiers critiques
  - Évaluer les vulnérabilités de l'annuaire central
  - Évaluer les défaillances potentielles d'un prestataire externe
  - Évaluer les vulnérabilités liées au partage des données inter-établissements
  - Évaluer les vulnérabilités des opérateurs de télémaintenance
  - Évaluer la vulnérabilité des dispositifs connectés et des outils collaboratifs
  - Hiérarchiser les mesures de protection en fonction des vulnérabilités
  - Intégrer le processus cumulatif de dysfonctionnement
  - Anticiper la mise en œuvre de contres mesures immédiates et évaluer l'impact

PARTIE 1 : Prévenir le risque numérique

Chapitre 2 : Formaliser un plan de mise en conformité adapté

- Formaliser des actions pour sécuriser le système d'information
- Des mesures prioritaires à mettre en œuvre

1.1 Les directives NIS : sécurité des réseaux et des systèmes d'information

- La directive Network and information System Security : NIS est adopté le 6 juillet 2016 par les institutions européennes
- Inscrit en droit français par la loi de transposition du 27 février 2018 et décret n° 2018-384 du 23 mai 2018, imposent des obligations aux 135 ES supports de GHT

1.2 La politique de sécurité des systèmes de l'information PSSI

- Chaque ES doit rédiger un document spécifique relatif à la politique de sécurité des systèmes d'information

> L'Agence du Numérique en Santé (ANS) est chargée de l'élaboration et la publication de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), cadre devant être respecté par tous les acteurs de la santé pour sécuriser les systèmes d'information de santé (SIS).

1.3 Le plan d'action de sécurité des systèmes d'information

- Recommandation de formaliser un plan d'action pour chaque ES.

  Si plusieurs sites : un plan spécifique et un socle commun sera rédigé
- Il est révisé tous les ans
- Il définit des mesures concrètes à mettre en œuvre avec un calendrier précis
- Il est adapté à chaque activité de soir ou support

1.4 Les 23 règles de sécurité des 135 ES Support de GHT

- 4 obligation pour ces ES
  - L'application des 23 règles de sécurité
  - La désignation d'un point de contact à l'ANSSI
  - La déclaration des systèmes d'information essentiels à l'ANSSI
  - La notification à l'ANSSI des incidents de sécurité sur venus

1.5 Définir les systèmes d'information essentiels

PARTIE 1 : Prévenir le risque numérique

Chapitre 2 : Formaliser un plan de mise en conformité adapté

- Formaliser des actions pour sécuriser le système d'information
- Des mesures prioritaires à mettre en œuvre

2.1 Le référentiel des 43 mesures prioritaires de sécurité des systèmes

Ces mesures sont décrites dans le référentiel à destination des établissements élaboré par la DGOS et disponible sur le site internet du ministère de la Santé et de la Prévention.

2.2 La gestion des correctifs de sécurité, une mesure prioritaire majeure

- Nécessité de formaliser une démarche qui vise à effectuer les mises à jour régulières sur les applications utilisées

2.3 Cloisonner l'architecture, une mesure prioritaire majeure

- Dès la conception de l'architecture réseau, il est important de raisonner par segmentation en zones composées de système devant répondre à des conventions de sécurité homogènes

2.4 Maitriser l'authentification des accès et des mots de passe

- La revue complète des comptes et des habilitations est une opération à effectuer annuellement
- La procédure de renouvellent automatique des mot de passe utilisateur et administrateur tus les 6 mois doit être mis en place.

2.5 Protéger la messagerie professionnelle

- Principal vecteur d'infection du poste de travail

→ Sensibilisation +++ des nouveaux arrivants et professionnels en poste

2.6 Des campagnes aléatoires de « phishing »

- Des campagnes aléatoires de « phishing » sont de bon leviers pour la sensibilisation

2.7 Identifier les données sensibles et les flux stratégiques

- Nécessité de repérer et protéger les donner sensibles
- Définir les mesures de sécurité spécifique pour les protéger

2.8 Le référentiel Identifiant National Santé : INS

- Il décrit les conditions et modalités de mise en œuvre de l'obligation de référencement des données de santé

Pour aller plus loin : le référentiel national de santé

2.9 La nécessité de mettre en œuvre des audits réguliers

- Permettre d'identifier les vulnérabilité au sein de l'ES
- Mise en place de mesures correctives ensuite

Fiche réflexe 2 : un plan de mise en conformité

- Mettre en œuvre le décret 2018 pour les OSE : sécurité des systèmes d'information
- Formaliser un plan de mise en conformité conforme à la PSSI
- Appliquer l'instruction dite « 309 »
- Suivre et mettre en œuvre les correctifs de sécurité
- Cloisonner l'architecture du système d'information
- Mettre en œuvre le référentiel des 43 mesures prioritaires
- Mettre en œuvre les 23 règles pour les établissements support de GHT
- Identifier les systèmes d'information essentiels
- Maîtriser les accès et les mots de passe du système d'information
- Protéger la messagerie professionnelle du personnel
- Réaliser des campagnes de « *phishing* »
- Maîtriser et sécuriser les données sensibles de l'établissement
- Mettre en œuvre le référentiel national de santé INS
- Assurer une veille : CERT-FR /CERT-SANTE sur les vulnérabilités logicielles
- Réaliser des audits réguliers du système d'information

PARTIE 2 : Elaborer le volet numérique

Chapitre 1 : Les modalités de mise en œuvre

- L'articulation avec les plans ORSAN, gestion des tensions, PCA, PRA
- Le volet numérique
- Coordonner et impliquer l'ensemble des acteurs
- Une cellule de crise : décision et opération
- La mobilisation des ressources techniques expertes
- Les étapes à suivre lors d'un incident numérique
-La conservation des preuves, le dépôt de plainte et la demande de rançon

1.1 Le plan ORSAN : un plan de réponse régional

- Déclenché par le DG ARS ou à la demande du préfet, il est décliné dans les ES dans leur plan de gestion des tensions et SSE
- La DTS « cyber sécurisation des ES » prend en compte le risque numérique comme une menace et risque majeur

A décliner par des mesures opérationnelles dans les plans de tensions et SSE

1.2 Le plan de gestion des tensions hospitalières

- Permet d'adapter rapidement les organisations internes face à un évènement
- Nécessité d'avoir un volet spécifique au risque numérique dans chaque référentiel

Le volet numérique décrit les mesures graduées activables en fonction de la nature, de l'ampleur et de la cinétique de l'incident numérique

1.3 Articulation avec les plans de continuité / reprise d'activité

- L'articulation se fera selon les procédures décrites dans
  - Le PCA
  - Le PRA

1.4 Le PCA du système d'information

- Décrit l'architecture de secours
  - Dédoublement de la salle des machines
  - Dédoublement du cœur réseau
  - Dédoublement des lignes réseaux
  - …
- Mise en place de procédures dégradées

1.5 Le PRA du système d'information

- Décrit les process à mettre en œuvre pour restaurer les équipements et applications métiers corrompus

PARTIE 2 : Elaborer le volet numérique

Chapitre 1 : Les modalités de mise en œuvre

- L'articulation avec les plans ORSAN, gestion des tensions, PCA, PRA
- Le volet numérique
- Coordonner et impliquer l'ensemble des acteurs
- Une cellule de crise : décision et opération
- La mobilisation des ressources techniques expertes
- Les étapes à suivre lors d'un incident numérique
-La conservation des preuves, le dépôt de plainte et la demande de rançon

2.1 L'intérêt de disposer d'un volet numérique

- Anticiper la formalisation d'un évènement
- Limiter l'impact numérique en cas d'incident
- Préparer une réponse proportionnée et adaptée à la situation

2.2 Un volet numérique qui pourra être mutualisé au sein du GHT

- Cette mutualisation peut être effectuée en lien avec l'ARS

2.3 Les critères de déclenchement du volet numérique

- Pas systématique à chaque incident, c'est un compromis des applications essentiels de l'ES, de la durée de l'évènement, avec un risque éventuel de perte de chance pour le patient
- Toujours à la demande du DG de l'ES

2.4 La confidentialité du volet numérique

- Ce volet doit être considéré comme CONFIDENTIEL
- Les informations et la mise en œuvre du volet doivent être protégées

PARTIE 2 : Elaborer le volet numérique

Chapitre 1 : Les modalités de mise en œuvre

- L'articulation avec les plans ORSAN, gestion des tensions, PCA, PRA
- Le volet numérique
- Coordonner et impliquer l'ensemble des acteurs
- Une cellule de crise : décision et opération
- La mobilisation des ressources techniques expertes
- Les étapes à suivre lors d'un incident numérique
-La conservation des preuves, le dépôt de plainte et la demande de rançon

3.1 L'implication des acteur pour l'élaboration du volet

- Nécessité d'avoir un groupe chargé de la planification
  - Équipe chargée de la sécurité des systèmes d'information
  - Equipe SSE
  - Personnels médicaux et paramédicaux
  - P. CME
  - DS, RH
  - CHCST
  - Représentant services techniques et logistiques

3.2 La coordination par l'ARS

- L'ARS pourra déclencher en fonction de la gravité de l'évènement, la cellule de crise en interne
- L'ARS coordonnera des ressources techniques spécialisées

3.3 Un appui des agences nationales

- L'ES pourra s'appuyer sur les compétences de l'agence du numérique en santé

PARTIE 2 : Elaborer le volet numérique

Chapitre 1 : Les modalités de mise en œuvre

- L'articulation avec les plans ORSAN, gestion des tensions, PCA, PRA
- Le volet numérique
- Coordonner et impliquer l'ensemble des acteurs
- Une cellule de crise : décision et opération
- La mobilisation des ressources techniques expertes
- Les étapes à suivre lors d'un incident numérique
- La conservation des preuves, le dépôt de plainte et la demande de rançon

4.1 Un organe de pilotage de la crise numérique

- 2 niveaux indispensables
  - Volet décisionnel : avec le DG de l'ES, son P. CME et DMC pour la remontée des informations mais aussi les différentes fonctions nécessaires à la gestion de la situations en fonction des incidents sur la prise en charge des patients
  - Volet technique opérationnel : compétences techniques de l'ES qui pourra avoir contact notamment avec l'ANSSI si nécessaire

4.2 Le Directeur médical de crise

- Il organise le flux des patients en lien avec la Cellule de crise

4.3 Le rôle de la cellule de crise

- Elle est chargée de :
  - Centraliser l'ensemble des informations
  - Mesurer l'impact sur la prise en charge de patients
  - Valider les action à mettre en œuvre pour permettre la continuité d'activité
- Contact permanent de l'ARS, du SAMU via le DMC
- Mise en place d'un journal de bord
- Prévoir une communication extérieure possible

4.4 La cellule de crise communique en interne

- La communication interne permet d'informer en temps réel les professionnels

4.5 La logistique nécessaire à la cellule de crise

- Salle avec connexion internet avec lignes téléphoniques fonctionnelles même en cas d'avaries sur le réseau principal
- Moyens de communication spécifiques en cas de coupure des moyens habituels
- Annuaires téléphoniques (versus papier)

4.6 un vecteur de communication rapide et sécurisé

- Nécessité de prévoir une organisation de communication rapide via une application externe pour permettre les échanges qui ne sont pas du secret professionnel

PARTIE 2 : Elaborer le volet numérique

Chapitre 1 : Les modalités de mise en œuvre

- L'articulation avec les plans ORSAN, gestion des tensions, PCA, PRA
- Le volet numérique
- Coordonner et impliquer l'ensemble des acteurs
- Une cellule de crise : décision et opération
- La mobilisation des ressources techniques expertes
- Les étapes à suivre lors d'un incident numérique
-La conservation des preuves, le dépôt de plainte et la demande de rançon

5.1 Des ressources techniques d'intervention

- Nécessité de préparer en amont des moyens opérationnels adaptés aux scénarii
- Disposer d'une équipe dédiée mobilisable des les premières minutes
- Liste mise à jour très régulièrement

5.2 Une équipe « réponse à l'incident » au sein du GHT

- En lien avec l'ARS, réflexion pour mutualiser au sein d'un GHT des experts qui pourront intervenir sur les différents sites
- Définir les rôles et places de chacun en cas de mobilisation sur un autre site (professionnels du site / professionnels externes)

5.3 L'appui de l'ANS et l'ANSSI

- Selon les capacités de mobilisation, l'ANS et l'ANSSI répondront aux sollicitations faites par les ES sur un évènement

PARTIE 2 : Elaborer le volet numérique

Chapitre 1 : Les modalités de mise en œuvre

- L'articulation avec les plans ORSAN, gestion des tensions, PCA, PRA
- Le volet numérique
- Coordonner et impliquer l'ensemble des acteurs
- Une cellule de crise : décision et opération
- La mobilisation des ressources techniques expertes
- Les étapes à suivre lors d'un incident numérique
-La conservation des preuves, le dépôt de plainte et la demande de rançon

6.1 Des mesures de gestion adaptées à la nature de l'incident numériques

- Les expertises doivent être adaptés à chaque typologie et nature de l'attaque
- Selon le niveau de gravité, il ne sera peut être nécessaire que de déployer les premières étapes :
  - Détection
  - Qualification de l'évènement
  - Confinement
  - Eradication
- Ou le process dans sa globalité si l'évènement est majeur

PARTIE 2 : Elaborer le volet numérique

Chapitre 1 : Les modalités de mise en œuvre

- L'articulation avec les plans ORSAN, gestion des tensions, PCA, PRA
- Le volet numérique
- Coordonner et impliquer l'ensemble des acteurs
- Une cellule de crise : décision et opération
- La mobilisation des ressources techniques expertes
- Les étapes à suivre lors d'un incident numérique
-La conservation des preuves, le dépôt de plainte et la demande de rançon

7.1 La collecte des preuves des systèmes attaqués

- Ne surtout pas détruire de preuves qui serviront aux enquêteurs
- Récolter au fur et à mesures les différents éléments qui pourront servir pour la CNIL

7.2 Le dépôt de plainte

- A effectuer rapidement après l'incident auprès de la police nationale ou de la gendarmerie dans les 24 à 48h.

7.3 La gestion de demande de rançon

- NE PAS NEGOCIER avec l'assaillant
- Paiement EXCLU car n'empêche rien …

Fiche réflexe 3 : Modalités de mises en œuvre du volet numérique

- Élaborer un volet numérique
- Adapter le volet numérique à la nature de l'incident numérique
- Anticiper les mesures de gestion en fonction du type d'établissement
- Mettre en œuvre un volet numérique qui pourra être mutualisé au sein du GHT
- Corréler les mesures à mettre en œuvre avec le plan de continuité/reprise d'activité
- Se préparer au regard de l'impact sur l'offre de soins
- Définir des critères de déclenchement du volet numérique
- S'assurer de la confidentialité des mesures du volet numérique
- Impliquer la gouvernance interne à l'établissement pour l'élaboration du plan
- Organiser par anticipation la cellule de crise : membres, rôles et missions
- Organiser la logistique de la cellule de crise : téléphone, internet, liste des contacts
- Anticiper des moyens sécurisés de communication rapide type « groupe »
- Évaluer la possibilité de créer une équipe « réponse à incident »
- Définir le rôle/missions de l'équipe « réponse à incident »
- Définir des modalités de coordination avec l'ARS et le GRADeS
- Anticiper les échanges avec les experts nationaux (ANSSI, CERT-FR…)
- Anticiper l'appui de l'ANSSI et de l'ANS (liste des contacts)
- Anticiper les étapes à suivre pour restaurer un système d'information
- Anticiper la conservation des preuves, le dépôt de plainte

PARTIE 2 : Elaborer le volet numérique

Chapitre 2 : Les éléments généraux à préparer

- Les éléments de préparation généraux
- Les travaux préparatoires à la communication
- Le signalement interne d'une anomalie
- La procédure de signalement des incidents numériques
- Une veille sur les scénarii et vecteurs d'attaque fréquents

1.1 Des travaux d'anticipation

- Il est fondamental d'élaborer une stratégie claire d'actions précises à mettre en œuvre après un incident confirmé afin d'éviter :
  - La confusion
  - Les retards
  - Une mauvaise hiérarchisation des priorités
- Il faut aussi faire le lien avec les travaux de préparation déjà engagés en cas de SSE

1.2 Une réponse adaptée aux principaux scénarii

- Nécessité de se baser sur des évènements récents afin de prévoir les moyens techniques les plus adaptés possibles
- Mise à jour régulière des scénarii

1.3 Une stratégie de réponse commune en GHT

- Réponses préexistantes au sein du même GHT
- Connues et testées au sein des ES composant le GHT

1.4 Une description de l'offre de soins et des PEC à risque

- Nécessité d'une équipe dédiée composée de ressources médicales et paramédicales qui pourra recenser les services hébergeurs des patients à risque
- Disposer de procédure permettant :
  - L'évaluation des sorties anticipables
  - D'étudier la pertinence d'annulation d'hospitalisations programmées
  - D'identifier les patients dont l'hospitalisation peut être différée

1.5 Un stock stratégique idéalement mutualisé

- Identifier les moyens dont dispose l'ES pour faire face à une SSE
- Contractualiser avec un opérateur des matériels et équipements nécessaires
- Permettre la construction d'une bulle sécurisée des applications indispensable au fonctionnement des soins critiques
- Mutualiser le matériel au sein du GHT et favoriser sa mobilisation 24/24

1.6 L'obligation de réaliser des exercices

- L'objectif d'un tel exercice est de tester la résilience de l'ES :
  - La chaîne d'alerte et le dispositif de crise ;
  - Les outils et les procédures existantes liés à la gestion des incidents et des crises ;
  - La coordination entre la gestion des équipes cybersécurité et l'impact sanitaire ;
  - La communication de crise interne/externe de la cellule de crise ;
  - La coordination de la cellule de crise avec le niveau régional et les autorités ;
  - La capacité des structures à travailler sans système d'information.

1.7 Des tests d'intrusion pour évaluer la sécurité globale

- Les tests d'intrusion sont un excellent moyen d'identifier les failles physiques et numérique

POUR ALLER PLUS LOIN :

- l'ANS propose des kits pratiques d'exercices avec 3 niveaux
- l'ANSSI propose un guide pour la réalisation d'un exercice cyber

PARTIE 2 : Elaborer le volet numérique

Chapitre 2 : Les éléments généraux à préparer

- Les éléments de préparation généraux
- Les travaux préparatoires à la communication
- Le signalement interne d'une anomalie
- La procédure de signalement des incidents numériques
- Une veille sur les scénarii et vecteurs d'attaque fréquents

2.1 Des outils de communication à préparer

- Anticipation et préparation en amont des outils et procédures de communication
- Les contenus des premiers communiqués doivent être prêt que soit à destination du grand public comme de la tutelle

Guide communication en cas de cyber de l'ANSSI

2.2 La communication interne

- Diffuser régulièrement des messages d'information auprès des professionnels pour rassurer et identifier l'évolution
- Des canaux alternatifs doivent être envisagés en amont d'une crise en cas d'impossibilité de mails ….

2.3 La communication externe

- Concertation étroite avec l'ARS et l'ES. C'est l'ARS qui communique vers les ES voisins
- Nécessité de n'avoir qu'une personne identifiée pour la communication avec les médias

2.4 Un dispositif d'information auprès des patients et familles

- Préparation d'un dispositif d'information relatif à l'incident envers les patients et familles notamment en cas de violation de données de snaté
- Vigilance accrue sur le secteurs de pédiatrie et néonatalogie

2.5 Les moyens alternatifs de communication

- Identifier des solutions de communication alternatives sau sein de l'ES
- Ces solutions devront être certifiées par l'ANSSI

PARTIE 2 : Elaborer le volet numérique

Chapitre 2 : Les éléments généraux à préparer

- Les éléments de préparation généraux
- Les travaux préparatoires à la communication
- Le signalement interne d'une anomalie
- La procédure de signalement des incidents numériques
- Une veille sur les scénarii et vecteurs d'attaque fréquents

3.1 Le signalement d'une anomalie du système d'information

- Procédure d'alerte efficiente y compris ela nuit et le WE permettant de diffuser sans délai l'information à l'équipe technique en charge du système d'information
- Définir les mesures à prendre à la réception de l'alerte
- Nécessité d'avoir des circuits de remontées d'information les plus courts possibles

3.2 Définir des critères d'alertes internes

- Incident parfois difficiles à identifier et à caractériser
- Nécessité de mettre en place en amont une organisation interne d'alerte que les professionnels doivent connaitre avec une vigilance aux nouveaux arrivant, intérimaire …

PARTIE 2 : Elaborer le volet numérique

Chapitre 2 : Les éléments généraux à préparer

- Les éléments de préparation généraux
- Les travaux préparatoires à la communication
- Le signalement interne d'une anomalie
- La procédure de signalement des incidents numériques
- Une veille sur les scénarii et vecteurs d'attaque fréquents

4.1 Informer le personnel pour sécuriser le système d'information

- Dès la confirmation de l'incident, une communication interne rapide sera nécessaire pour confirmer et protéger l'ensemble du système d'information et assurer aussi sa sauvegarde
- Il est donc indispensable d'avoir une procédure définie pour informer le personnel
- Cette procédure doit être possible ne cas absence du système d'information

4.2 Le cadre réglementaire du signalement d'un incident numérique

- Décret n°2016-1214 du 12 septembre 2016oblige les ES à déclarer les incident via un portail de signalement. Ceci permet aussi à l'ARS d'anticiper l'offre de soins
- Les ES OSE ont obligation de déclarer auprès du CERT-FR afin d'éviter la propagation sur d'autres ES
- Si des données personnelles sont impactées l'ES devra déclarer l'incident aussi à la CNIL dans les 72h

4.3 Le signalement aux autorités compétences

- **Signalement auprès du portail conformément à l'article L.1111-8-2 du CSP**
  - https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil
  - La déclaration au portail déclenche le signalement au CERT

- **Signalement auprès du CERT-FR (ANSSI)**
  - Disponible 7j/7, 24h/24, Téléphone au +33 (0)1 71 75 84 68.
  - cert-fr.cossi@ssi.gouv.fr

- **Signalement auprès du CERT-SANTE (ANS)**
  - Disponible 7j/7, 24h/24 ; Téléphone au +33 (0)9 72 43 91 25
  - https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil

- **Signalement sur le site de la CNIL**
  - En cas de fuite de données personnelles, il faut signaler la cyberattaque à la Commission nationale de l'informatique et des libertés (CNIL) dans les 72h suivant sa constatation, conformément à l'article 33 du règlement général sur la protection des données (RGPD).
  - Un formulaire est téléchargeable sur le site Internet de la CNIL.
  - https://www.cnil.fr/fr/les-violations-de-donnees-personnelles

- **Signalement auprès du point focal régional (gestion de crise) de l'ARS**
  - L'ARS reçoit notification du dépôt du signalement sur le portail des signalements, sur la BAL, et le retransmet en interne au référent des systèmes d'information, au service chargé de la gestion de crise et à la direction métier concernée.

4.2 Les éléments à recueillir lors d'un évènement

- Préparer en amont une trame d'information à recueillir avec notamment des éléments sur la gravité de l'incident, son périmètre
- Les autres éléments à communiquer :

  - L'impact sur le fonctionnement des systèmes d'information de l'établissement ;
  - L'impact estimé sur la continuité des prises en charge médicale ;
  - Les besoins d'appui en ressources techniques spécialisées ;
  - Les besoins d'appui pour assurer la continuité des soins ;
  - Relais de l'ARS pour informer/communiquer auprès d'autres opérateurs de soins (établissements de santé, établissements médico-sociaux, laboratoires d'analyses, professionnels de santé libéraux, transporteurs sanitaires, cabinets de radiologie...).

PARTIE 2 : Elaborer le volet numérique

Chapitre 2 : Les éléments généraux à préparer

- Les éléments de préparation généraux
- Les travaux préparatoires à la communication
- Le signalement interne d'une anomalie
- La procédure de signalement des incidents numériques
- Une veille sur les scénarii et vecteurs d'attaque fréquents

5.1 Une veille permanente sur les typologies d'attaque

- Sur les modes opératoires liés aux cyberattaque
- Pas toujours visible instantanément (plusieurs heures avant de découvrir les premiers effets)

5.2 Les vecteurs d'attaque fréquents

- Hameçonnage ou « phishing » permet d'obtenir des données personnelles
- Ransomware : logiciel placé dans une pièce jointe de mail. C'est cette attaque que subissent essentiellement les ES
  - Le but est de bloquer l'accès à votre ordinateur
- Faiblesse structurelle sur les annuaires de la structure
- Parfois cela peut aussi provenir en départ par l'un des prestataire

5.3 L'acte de malveillance

- Possibilité d'être initié par un personnel interne à l'ES

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités

LA stratégie de sauvegarde pour anticiper l'étape de restauration

- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

1.1 Détecter et reconnaitre une perturbation informatique

- Le personnel de l'ES peut lui-même reconnaitre ou détecter une défaillance sur le réseau
- Mais les cyber attaques sont difficile à identifier et à caractériser car elles peuvent passer par des dysfonctionnements mineurs voire inaperçus
- Il faut déterminer le type d'attaque rapidement afin de choisir la réponse à mettre en œuvre

1.2 La mise en place d'outils de détection efficaces

- Nécessité de mettre en place des analyses régulières ou continues du processus de sécurité numérique interne à l'ES
- Vigilance humaine +++

1.3 Vérifier la capacité de détecter des codes malveillants

- Nécessité d'interroger régulièrement l'ES sur sa capacité de détection

1.4 Evaluer la pertinence de mettre en œuvre la technologie EDR

- Outils de détection de réponses EDR (Endpoint Detection Response) réponde aux objectifs de détection d'attaque inconnues, de lancement de correctifs automatiques contre ces menaces. Une analyse comportementale du code malveillant est réalisée
- C'est une technologie qui complète le stratégie « antivirus » existante
- Surveille en permanence les informations relatives aux menaces
- Solution devant être mise en regard des ressources cyber à mobiliser
- Requiert sa remise à niveau pour prendre en compte les fonctionnalités nouvelles

1.5 Identifier le périmètre et le chemin de compromission suivie

- Après l'alerte, il faut obtenir le plus de détails possible sur le périmètre de l'attaque, le chemin de compromission, les vecteurs potentiels d'infection et les fonctions malveillantes

1.6 Collecter les journaux d'incident des éléments de sécurité

- Prévoir en amont une organisation permettant de recueillir du service identifié comme étant à l'origine de l'intrusion, les journaux d'incident dont les antivirus et les VPN
- Etape essentielle permettant de mettre en place la meilleure stratégie de confinement et de continuité d'activité

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités

LA stratégie de sauvegarde pour anticiper l'étape de restauration

- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

2.1 Identifier les systèmes corrompus

- Le nombre de postes administrateurs, nombre de postes utilisateurs, nombre de serveurs, type de système touchés …

  → niveau de gravité de l'incident

- Faire régulièrement des exercices pour déterminer rapidement les systèmes corrompus

2.2 Contrôler l'intégralité des sauvegardes

- Prioritairement s'assurer que les sauvegardes régulièrement réalisées soient ou pas corrompues
- Anticipation de ce contrôle
- Suspendre toute sauvegarde le temps que l'intrusion n »est pas identifiée

2.3 La qualification va déterminer le déclenchement du volet numérique

- Pour cela il faut qualifier précisément le type d'incident, sa gravité, les vecteurs potentiels les fonctions malveillantes, le périmètre …

  → le maintien de la qualité et la sécurité des oins est la priorité

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités

LA stratégie de sauvegarde pour anticiper l'étape de restauration

- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

3.1 Le confinement des systèmes corrompus pour endiguer l'attaque

- Contenir l'incident à un périmètre restreint
- Le confinement est une prise de décision qu'il faut anticiper, de par ces conséquences

3.2 Des stratégies de confinement différentes selon le type d'incident

- Nécessité de préparer des stratégies de confinement distincts pour chaque type d'incident majeur, avec des critères clairement documentés pour faciliter la prise de décision

3.3 Des mesures immédiates pour réduire la surface d'attaque

- Nécessité de mettre en œuvre des mesures immédiates pour endiguer l'attaque mais celle-ci doivent être anticipées selon la classification de l'attaque
- Selon la typologie de l'attaque, il faudra :

  - Déconnecter immédiatement tous les appareils compromis : isoler du réseau et du système de stockage ;
  - Éteindre tous les appareils qui n'ont pas été infectés afin de limiter les dommages ;
  - Déconnecter les unités de stockage externe ;
  - Lancer une analyse antivirale.

Pour aller plus loin, une fiche réflexe ANS : Réagir à un acte de malveillance.

Pour aller plus loin, une fiche réflexe ANS : Agir contre un maliciel.

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités

LA stratégie de sauvegarde pour anticiper l'étape de restauration

- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

4.1 Des mesures temporaires à mettre en œuvre

- Impacter le moins possible les services de soins et administratifs : faire préciser aux services de soins les niveaux de services attendus et les durées maximales admissibles
- Communication préalable pour préciser le cadre d'utilisation d'outils temporaires

4.2 Des infrastructures temporaires

- Ordinateurs portables, dispositif mobiles d'accès à internet, téléphone mobiles, supports externes
- Clés 4G/5G (location ponctuelle ? Prêt ?)

4.3 Une vigilance à la saturation du réseau

- Lors de la mise en place du réseau temporaire, une vigilance accrue doit être portée à la saturation probable de ce réseau

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités

LA stratégie de sauvegarde pour anticiper l'étape de restauration

- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

5.1 La suppression des codes malveillants

- L'éradication peut être nécessaire pour éliminer les composants corrompus : suppression de codes, désactivation de comptes utilisateurs piratés
- L'équipe en charge de l'éradication doit consigner l'ensemble des actions mises en œuvre

5.2 La correction des vulnérabilités

- Dans le système qui a permis l'intrusion : mise à jour logicielles, reconfiguration des paramètres réseau, remplacements des systèmes obsolètes
- Mise en place de nouvelles règles de sécurité avec entre autre modification des mots de passe des comptes

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités
- La stratégie de sauvegarde pour anticiper l'étape de restauration
- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

6.1 Des sauvegardes déconnectées du système d'information

- Identifier et restaurer la version la plus récentes des données sauvegardées
- Des sauvegardes régulières doivent être réalisée s surtout en soins critiques et elles doivent être déconnectées du système d'information pour prévenir leur chiffrement

⇨ stockage à froid (protection des sauvegardes d'une destruction)

6.2 Une attention particulière pour les données et applications critiques

- Dupliquer les informations essentiels des applications utilisées

  - Les données : serveurs, postes utilisateur ;
  - Application métier bloc opératoire : planning des interventions ;
  - Application métier imagerie : planning des examens ;
  - Les applications : sauvegarde des applicatifs métiers ;
  - Sauvegarde d'un système d'exploitation / reconstruction rapide d'un serveur ;
  - Les éléments d'infrastructure : sauvegarde du paramétrage d'éléments d'infrastructures.

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités
- La stratégie de sauvegarde pour anticiper l'étape de restauration
- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

7.1 L'application du plan de reprise d'activité PRA

- Définir pour chacune des applications métiers, dans un contexte métier donné, les étapes à suivre lors du processus de restauration suite à un incident majeur
- Déterminer quelles sont les données et les logiciels qui devront etre restaurés dans quelles conditions

7.2 Restaurer les systèmes et données endommagées

- S'effectue à partir des sauvegardes saines mais peut nécessité des modifications importantes pour sécuriser les outils et limiter le risque d'une nouvelle attaque
- Besoin accru de RH pour ce processus qui peut être long mais indispensable
- Phase à planifier et à adapter aux besoins spécifiques de chaque ES

7.3 Des tests de restauration éprouvés et testés

- Une phase tests est nécessaire pour vérifier si les applications métiers restaurées fonctionnent normalement après l'incident

  ⇨ des exercices test de restauration doivent être réalisés tous les ans pour vérifier les séquences de restauration

7.4 La restauration des applications, un processus pouvant être long

- Le processus global de restauration peut durer plusieurs mois, il est donc in pensable de s'être préparer à tenir dans la durée

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités
- La stratégie de sauvegarde pour anticiper l'étape de restauration
- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

8.1 La phase de reconstruction

- Plusieurs scénarii de reconstruction peuvent être proposés en fonction de l'ampleur de l'incident et de la complexité de l'attaque
- Mais il faut garantir la continuité des prises en charges

8.2 Le choix de reconstruire les applications au sein d'une zone sécurisée

- Il peut être utile de reconstruire en zone isolée et donc d'acquérir de nouvelle infrastructures et des matériels neufs

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités
- La stratégie de sauvegarde pour anticiper l'étape de restauration
- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

9.1 Définir les critères de sortie de crise

- Etape importante dans le processus de gestion de crise
- Mais l'ES n'est pas forcément revenu à son fonctionnement optimal, cela traduit juste que les activités essentielles ont repris

9.2 Arbitrer la suppression du fonctionnement dégradé

- Etape longue pouvant durer plusieurs mois
- Permet d'arbitrer le maintien ou la suppression des solutions de contournement et réévaluer la mobilisation des effectifs en charge des systèmes d'information

PARTIE 2 : Elaborer le volet numérique

Chapitre 3 : Se préparer aux étapes à suivre

- La détection et l'identification du périmètre de la cyberattaque
- Le recensement des systèmes corrompus et la qualification de l'incident
- Le confinement des zones affectées pour réduite la surface de l'attaque
- Le fonctionnement du système d'information en mode dégradé
- L'éradication par la correction des vulnérabilités
- La stratégie de sauvegarde pour anticiper l'étape de restauration
- La restauration des systèmes d'information corrompus
- La reconstruction des systèmes compromis
- Arbitrer la sortie de crise
- Effectuer un retour d'expérience post attaque

10.1 Analyser les forces et les faiblesses

- Partie intégrante du processus pour réduire les risques de futures attaques et mieux protéger les patients pris en charge
- Réflexion partagée avec tous les intervenants pour analyser les forces et faiblesses montrées par le dispositif, le schéma de l'alerte, les modalités de mobilisation des RH et matériels

10.2 Tirer les enseignements

- Prévenir les attaques similaires, les conclusions du ReTEX doivent servir +++
- Implication de revoir le rôle et els responsabilités, mettre à jour le plan de communication

S'entourer de personnes neutres pour faciliter le Retex

10.3 Une communication à adapter lors des retex

- Attention aux retex public, ils doivent toujours être validés par la cellule communication de l'ARS

Fiche réflexe 4 : Les travaux de préparation du volet numérique

- Disposer d'une astreinte 24h/24 sur la sécurité numérique
- Sensibiliser les personnels au risque numérique et numéros d'astreinte
- Adapter un plan de réponse adapté aux différents scenarii
- Disposer d'une documentation rapidement accessible
- Disposer d'une stratégie de réponse mutualisée au sein du GHT
- Réaliser une cartographie de l'offre de soins et des activités à risque
- Mobiliser des moyens, constituer un stock stratégique au niveau GHT/région
- Préparer des modèles à utiliser pour la communication interne et externe
- Anticiper des moyens alternatifs pour communiquer (interne/externe)
- Former les équipes d'intervention informatique aux différents scenarii d'un incident
- Définir des critères d'alertes internes d'un incident numérique pour le personnel
- Définir une procédure pour informer rapidement le personnel
- Définir une procédure pour signaler l'incident aux autorités compétentes
- Savoir reconnaître une perturbation, mettre en place des systèmes de détection efficace
- Évaluer la capacité de l'établissement à mieux détecter les actions malveillantes
- Savoir qualifier l'incident, le périmètre, les vecteurs d'attaque, les systèmes compromis
- Définir une stratégie de sauvegarde, positionner les sauvegardes hors du SI
- Préparer le confinement, mesures immédiates réduire la surface d'attaque
- Préparer la phase d'éradication par la correction des vulnérabilités
- Disposer d'une méthodologie de restauration des systèmes corrompus
- Disposer d'une procédure permettant le report des hospitalisations non critiques
- Mettre en place des infrastructures temporaires pour permettre le mode dégradé
- Conserver les preuves, dépôt de plainte, demande de rançon
- Réaliser régulièrement des exercices de crise et en tirer des enseignements

PARTIE 3 : L'organisation des soins

Chapitre 1 : L'impact sur l'organisation des soins

- Le pilotage de la continuité des soins
- L'organisation des soins en mode dégradé
- Les procédures du mode dégradé et les exercices
- Le soutien nécessaires aux équipes

1.1 Le pilotage de l'ARS

- Pilotage robuste et indispensable par l'ARS
- La cellule de crise ARS doit avoir en temps réel des capacités d'accueil et de prise en charge territoire, capacité d'hospitalisation avec un focus sur les lits de soins critiques adulte et enfant
- Utilisation des outils d'organisation des GHT

1.2 Organiser la continuité des soins avec les ES du territoire

- Nécessite des travaux préparatoires pour l'accueil de patients et éventuellement des professionnels chargés de leur suivi
- L'ARS déclenche la DST « évacuation des ES et EMS »
- L'ES doit s'appuyer sur son annexe « stratégie de déprogrammation et de reprogrammation » de son plan de gestion de crise

1.3 Vérifier la capacité d'admission de nouveaux patients

- Quantifier la capacité de l'ES à accueillir de nouveaux patients en adoptant une réflexion par filière de soins.
- Lister par service et spécialité les motifs de recours à l'hospitalisation qui pourraient être différée sans préjudice
- Définir les limite capacitaire donc le seuil à partir duquel il sera nécessaire de faire appel à d'autres ES

1.4 Choisir de transférer certains patients vers d'autres ES

- Sous pilotage et coordination de l'ARS
- Nécessité de bien définir les patients pouvant supporter le transfert

1.5 Quantifier en continue l'impact sur la qualité et la sécurité des soins

- Nécessité de prendre en compte ce sujet dans le plan de gestion des SSE avec mobilisation de la CCH toujours en lien avec le volet numérique

PARTIE 3 : L'organisation des soins

Chapitre 1 : L'impact sur l'organisation des soins

- Le pilotage de la continuité des soins
- L'organisation des soins en mode dégradé
- Les procédures du mode dégradé et les exercices
- Le soutien nécessaires aux équipes

2.1 Le réseau téléphonique et la messagerie

- Prévoir des modalités de fonctionnement dégradé et notamment de formaliser un plan de continuité d'activité

2.2 La gestion du poste de travail : déconnecter et éteindre son PC

- Rappel réguliers envers les professionnels :
  - Éteindre son PC le sort,
  - Se déconnecter lors qu'on s'absente
  - Se déconnecter d'internet quand non nécessaire

2.3 L'offre de soins

- Impact sur la prise en charge des patients autour des différents logiciels utilisés pour leur soins :

  - Panne du réseau téléphonique (standard inaccessible) et de la messagerie ;
  - Impossibilité de contacter le SAMU-Centre 15 ;
  - Planning du bloc opératoire indisponible ; visualisation des images au bloc indisponible ;
  - Dossier patient informatisé inaccessible ;
  - Gestion du patient perturbée : admissions, étiquettes patients, certificats de décès ;
  - Logiciel métier non fonctionnel (imagerie, pharmacie, laboratoire…) ;
  - Centrale de monitorage non fonctionnel (moniteur multiparamétrique, ventilateur…) ;
  - Panne du réseau GTC (chauffage, climatisation, traitement d'air…) ;
  - Demande d'examens d'imagerie, de laboratoire indisponible ;
  - Rendu de résultats de biologie, compte rendu d'examen, accès à l'historique des examens indisponible ;
  - Arrêt des séances de radiothérapie, de chimiothérapie ;
  - Disparition des plannings de rendez-vous et plans des lits ;
  - Absence de traçabilité à la stérilisation ;
  - Etc.

2.4 Les dispositifs médicaux

- Les centrales de surveillance peuvent être impactées par une cyber attaque, il est donc nécessaire d'y penser et de voir comment fonctionner en mode dégradé

  ⇨ Recommandation ANSM « Cybersécurité des dispositif médicaux »

2.5 Les fonctions logistiques

- Une vigilance accrue doit être portée sur toutes la logistique : distribution des médicaments, stérilisation, distribution des repas, le linge, la gestion des déchets, ….

  ⇨ un mode dégradé doit être prévu et connu des professionnels

2.6 La gestion centralisée /technique des bâtiments

- Gestion de tous les systèmes de contrôle : traitement d'air dans les différents services (bloc …), accès aux bâtiments, ascenseurs, groupes électrogènes

  ⇨ contre-mesures obligatoires de fonctionnement en mode dégradé

2.7 La gestion administrative

- Prévoir un mode dégradé pour la gestion des codage d'actes, la facturation, la gestion RH, la paie …

PARTIE 3 : L'organisation des soins

Chapitre 1 : L'impact sur l'organisation des soins

- Le pilotage de la continuité des soins
- L'organisation des soins en mode dégradé
- Les procédures du mode dégradé et les exercices
- Le soutien nécessaires aux équipes

3.1 Des procédures du mode dégradé et les exercices

- Anticiper la stratégie du fonctionnement en mode dégradé par ordre de priorité selon les différents typologies d'attaque
- Un cahier de procédures opérationnels imprimes doit être mis dans les services pouvant être concernés

3.2/3.3 Des procédures connues et testées grâce à des exercices réguliers

- Chaque service qui utilise des applications logicielles métiers critiques doit continuer à travailler : nécessité de s'approprier les procédures dégradées définies
- Dans la préparation du fonctionnement dégradé, il faut s'assurer que les procédures soient connues

3.4 Une agilité des services de soins

- Les services doivent pouvoir fonctionner ne mode dégradé quasi instantanément grâce à la connaissance des procédures

PARTIE 3 : L'organisation des soins

Chapitre 1 : L'impact sur l'organisation des soins

- Le pilotage de la continuité des soins
- L'organisation des soins en mode dégradé
- Les procédures du mode dégradé et les exercices
- Le soutien nécessaires aux équipes

4.1 Veiller au soutien des équipes

- Lors d'une cyberattaque, il faut faire preuve de réactivité mais aussi prendre du recul pour garantir le bon déroulement des plans de réponse, canaliser les énergie et les inquiétudes, mettre en place tous les moyens nécessaire pour gérer au mieux la situation

PARTIE 3 : L'organisation des soins

Chapitre 2 : La prise en charge en mode dégradé

- L'identification des activités critiques
- La prise en charge des patients en mode dégradé

1.1 Des modalités d'organisation en fonction des composants affectés

- Le fonctionnement en mode dégradé peut être différent selon les composants du système d'information impacté
- Plusieurs évènement peuvent nécessité ce passage en mode dégradé :
  - Application métier inaccessible
  - Messagerie indisponible
  - Serveur de base de données patients inaccessible
  - Dossier patient informatisé inaccessible

1.2 L'identification des services de soins critiques

- En amont la liste des activités critiques, les processus logistiques clés impactés et les modalité du mode dégradés doivent être parfaitement préparés
- Ces modalités de fonctionnement dégradé doivent préciser les niveaux de services minimum indispensables

PARTIE 3 : L'organisation des soins

Chapitre 2 : La prise en charge en mode dégradé

- L'identification des activités critiques
- La prise en charge des patients en mode dégradé

2.1 Le dossier patient informatisé

- Mettre en place avec l'éditeur du logiciel une procédure dégradée afin de pouvoir accéder, grâce à une sauvegarde des données DPI, en complète indépendance du système d'information
- Prévoir la possibilité d'imprimer par l'intermédiaire d'un ordinateur les prescription et plan de soins à minima

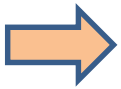
2.2 Le PC de sauvegarde

- Ce PC :

  - Doit fonctionner sur la chaîne de distribution électrique de secours de l'établissement ;
  - Doit être un poste de travail dédié à la procédure dégradée ;
  - Doit être connecté à une imprimante de façon directe (hors du réseau établissement) et disposer d'un toner de rechange ;
  - Doit disposer d'une procédure synthétique décrivant les modalités d'édition du dossier papier ;
  - Doit disposer d'un accès sécurisé ;
  - Doit disposer d'une fréquence et de modalités de sauvegarde sur un disque dur.

2.3 Le SAS et le SAMU-Centre 15

- Outil informatique incontournable
- Nécessité d'une interconnexion avec l'ARS, les SIS et les transports sanitaires
- Évaluer la nécessité de délester tout ou partie du flux téléphonique entrant par le Centre 15 vers les autres centre 15
- Actions a mener prioritairement :
  - Informer le SAMU zonal pour permettre une régulation vers d'autres établissements ;
  - Activation de la procédure d'entraide en lien avec l'ARS ;
  - Mobilisation du SMUR pour procéder à d'éventuels transferts.



Le centre 15 sera en lien avec le CCH via le DMC

2.4 Sécurisation des communications des SAS et SAMU-Centre 15

- PRIORITE face à l'évènement numérique
- Démarche de décloisonnement et de concertation métier pour définir les procédure opérationnelles, études d'outils techniques nécessaires
- Sécurisation des lignes SAMU-Centre 15 avec les différents services de soins

2.5 L'accueil aux urgences

- Réfléchir à la réorientation des patients vers d'autres ES ou la médecine de ville si possible
- Actions à mener :
  - Utiliser la procédure dégradée (étiquette) ;
  - Récupérer les dossiers « PC de sauvegarde » ;
  - Pour les patients sortants, imprimer les documents du dossier.

2.6 Le bloc opératoire

- Selon l'étendue de l'incident, il est nécessaire de qualifier :
  - L'analyse bénéfices/risques des patients pour permettre la déprogrammation d'actes/ interventions ;
  - La capacité de transférer les interventions à risque ou complexes vers d'autres établissements ;
  - La possibilité de disposer de créneaux d'intervention au sein d'un bloc opératoire mis à disposition par un établissement de santé du territoire pour permettre la continuité des prises en charge dans des conditions de qualité et sécurité ;
  - La capacité de l'établissement d'accueil à intégrer les équipes médicales et paramédicales ;
  - La nécessité de préserver les capacités du bloc opératoire aux patients dont le pronostic ne permet pas le report sans perte de chance ;
  - Le maintien de l'activité de chirurgie conventionnelle hors urgence vitale.

2.7 La stérilisation des dispositifs médicaux

- Risque d'impact majeur car le processus métier est souvent garanti par une application métier dédié
- Envisager le fonctionnement en mode dégradé c'est :
  - Prévoir une sauvegarde régulière
  - Mettre en œuvre une traçabilité manuelle
  - Etape de de mise en laveur ou autoclave
  - Etape de recomposition
  - Expédition des boites selon la recomposition /validation composition
  - Logiciel du mode dégradé
  - Évaluer la possibilité de sous-traiter de façon temporaire

2.8 Les soins critiques : réa, soins intensifs et continus

- Prévoir une organisation dégradé pour le suivi de monitorage des patients, la supervision des alarmes des dispositifs médicaux avec la pertinence de mettre un PC sauvegarde
- Etre très vigilant à la continuité des communications (SAMU, pharmacie, Imagerie, EFS …)

2.9 L'imagerie médicale

- L'impact est majeur et se traduit par :
  - Indisponibilité de la téléphonie ;
  - Indisponibilité du système d'information hospitalier (SIH) donc de l'identité des patients ;
  - Indisponibilité du RIS (Système d'Information Radiologique) ;
  - Indisponibilité de l'outil « téléradiologie » notamment lors des demandes d'avis (grande garde de neurochirurgie par exemple)
  - Impossibilité d'accéder au planning des examens d'imagerie ;
  - Inaccessibilité du système d'archivage PACS (*Picture Archiving and Communication System*) ;
  - Indisponibilité de la dictée vocale ;
  - Indisponibilité du système d'envoi des CRI aux cliniciens en intra institution et à l'extérieur (retour aux CR papier obligatoire) ;
  - Impossibilité de facturer les examens.
- Il faut donc en mode dégradé prévoir :
  - des moyens de communications
  - Une possible interprétation des examens sur la console d'acquisition
  - Privilégier les examens prioritaires
  - Anticiper la construction d'un réseau local temporaire
  - Revoir la rédaction des comptes rendus d'examen
  - Sauvegarder les images

LE PCA IMAGERIE MEDICALE doit etre défini selon plusieurs scénarii

2.10 Le laboratoire de biologie médicale

- L'impact est majeur nécessitant l'identification des prélèvements par le mode « étiquette »
- Le mode dégradé prévoit :
  - De sécuriser le circuit du prélèvement
  - L'application métier
  - De garantir la continuité de fonctionnement
  - La communication des résultats
  - Et enfin le retour à la normal

2.11 La pharmacie à usage intérieur PUI

- Le mode dégradé prévoit :
  - De disposer de sauvegarde régulières sur un support déconnecté du réseau
  - De garantir la continuité de fonctionnement
  - De disposer d'une sauvegarde récente des applications métiers
  - De disposer de formulaires papier
  - Des moyens alternatifs de communication

2.12 L'actualisation des données recueillies lors du mode dégradé

- CONVERSER tous les documents utilisés et définir l'ordre de priorités des données à reprendre

Fiche réflexe 5 : organisation des soins en cas d'incident numérique

- Anticiper les modalités de fonctionnement en fonction de la nature de l'incident
- Prévoir une communication adaptée pour les patients / validée par la cellule de crise
- Imprimer les procédures du mode dégradé - informer les personnels
- Préparer un plan de continuité d'activité des fonctions logistiques : déchets, transport…
- Mettre en œuvre un mode dégradé pour les gestions GTC/GTB
- Anticiper l'indisponibilité de la gestion administrative et notamment de la gestion paie
- Réaliser des exercices réguliers du mode dégradé au sein des services critiques
- Prévoir la continuité d'activité de soins avec les établissements de santé du territoire
- Anticiper l'organisation à mettre en œuvre pour le transfert des patients
- Quantifier en continu l'impact du mode dégradé sur la qualité et la sécurité
- Vérifier la capacité d'admission de nouveaux patients en fonctionnement dégradé
- Anticiper les modalités d'accès au DPI en mode dégradé au sein des services de soins
- SAMU-centre 15 : Sécuriser la téléphonie, informer le SAMU Zonal, délestage à organiser
- Accueil Urgence : Prévoir modalités d'accès au DPI, enregistrement manuel, délestage
- Bloc opératoire : Préserver l'activité du bloc aux urgences vitales, délestage
- Transport : Evaluer la possibilité de mettre en place un service coursier interne
- Téléphonie : Prévoir des modalités de communication alternatives
- Communication « type groupe » rapide : Prévoir en amont une application sécurisée
- Stérilisation : Anticiper la sauvegarde, traçabilité manuelle, sous-traiter l'activité
- Monitorage centralisée : Anticiper une modalité de gestion des alarmes centralisée
- Soins critiques : mode dégradé DPI, prévoir l'accès au mode dégradé du logiciel métier
- Imagerie : Privilégier les examens prioritaires, interprétation sur console d'acquisition
- Anticiper la construction d'un réseau local temporaire au sein des services critiques
- Laboratoire : Privilégier les examens prioritaires
- Pharmacie : Privilégier les examens prioritaires

Outils et guides complémentaires

- Observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social 2022
- Guide relatif aux règles de sauvegarde des systèmes d'information de santé.
- Recommandations de l'ANSM précisent des éléments à mettre en œuvre : « Cybersécurité des dispositifs médicaux intégrant du logiciel ».
- « 13 questions pour être incollable en matière de cyber sécurité » publié par l'ANS
- l'ANS propose des kits pratiques (débutant, intermédiaire, avancé) pour réaliser des exercices de crise.
- Fiche réflexe ANS : Réagir à un acte de malveillance.
- Fiche réflexe ANS : Agir contre un maliciel.
- L'ANS propose une fiche réflexe « Sécurisation de l'accès à distance des prestataires ».