LA CYBERATTAQUE AU CENTRE HOSPITALIER DE WALLONIE PICARDE

QUENTIN VICO

AUXILIAIRE EN STÉRILISATION

TYPOLOGIE DE LA MENACE

- La cyberattaque est une 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.

ANSSI (agence nationale de la sécurité des systèmes d'information)

Qui ?

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

Comment :

- ordinateurs, serveurs, isolés ou en réseaux reliés ou non à internet
- équipements périphériques

Risques :

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

Cibles en fonction :

- dépendance à l'automatisation et au numérique
- retard en matière de cyber-sécurité
- insuffisance dans les procédures informatique

POURQUOI IMPACTER UNE INSTITUTION DE SOIN ?

Difficultés financières ⟶ moyens de protections alloués vulnérables face à de ce type d'attaque

Faible niveau de sécurité numérique et milieu par définition "ouvert" (vulnérabilité pour intrusion également physique).

Une multitude de systèmes d'informations, avec des équipements et des logiciels appartenant à de nombreux prestataires externes

Le Covid 19 = mise en place télétravail = augmentation de la surface d'attaque car moins de surveillance.

DIMANCHE 17 JANVIER 2021

COMMENT A-T-ON DÉCOUVERT LA CYBERATTAQUE ?

17h40

Un membre du personnel dans une unité de soins n'arrive pas à ouvrir son logiciel. Il éteint et rallume le PC et là écran noir …

Il contact la garde informatique

RÉACTION DE L'INSTITUTION QUELQUES HEURES PLUS TARD

- Plan d'urgences hospitalier déclenché
- Rappel entier du service informatique pour supervision 24/24h
- Réunion entre direction informatique et médicale
- Demande d'intervention de certains fournisseurs, certains spécialistes de la Computer Crime Unit de la police fédérale et une société de sécurisation digitale

CONSÉQUENCES DE L'ATTAQUE

- 80 serveurs informatiques sur 300 impactés
- Plus de téléphonie
- Intrusions dans les données du personnel et des patients
- Tous les programmes informatiques bloqués
- Connexions vers l'extérieur coupées
- Interruption de la totalité des chaînes logistiques, de production, de gestion …
- Interruption de l'intranet
- Réallocation des moyens pour gérer la crise et donc baisse de la productivité **> *Retour mode dégradé* <**

Une attaque de cette ampleur peut provoquer :

- A court terme : Nuire à l'image de l'institution.
- A Moyen terme : Perte de patientèle.
- A Long terme : Impact sur la crédibilité de gestion

LES IMPACTS AU CHWAPI

- Déviation du 112 dans les hôpitaux de proximité pour les cas les plus critiques
- Planning opératoire pour les interventions programmées annulé
- Certaines consultations reportées
- Application en urgences du mode "dégradé" à tous les services

LES IMPACTS EN STERILISATION

- Attente des consignes de la direction => Aucune activité pour l'instant => une partie du personnel renvoyé chez eux
- Travail en mode dégradé et traçabilité papier
- Mise en place d'un mode de communication avec le bloc => gsm privé

CONSÉQUENCE SUR LE TERRAIN

- Plus de mails ni de téléphonie
- Plus aucun outil de travail informatique
- Stress des collaborateurs
- Sentiment de révolte et d'incompréhension pour le personnel déjà très éprouvé par la crise covid

L'ORGANISATION EN STÉRILISATION

Mise en place du mode "dégradé"

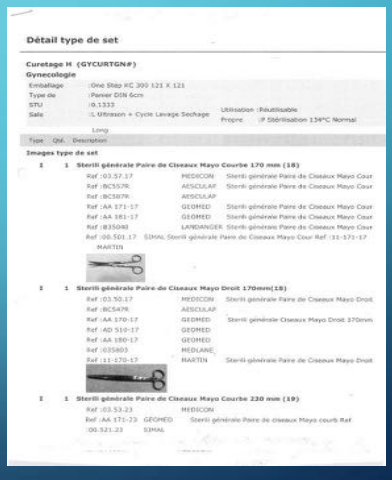
Vérification de la fonctionnalité du serveur externe "Satis" pour la surveillance des cycles des LDet des stérilisateurs

Prioriser des disciplines / sets

Listings papiers pour la recomposition des sets prioritaires (attention certains pas mis à jour)

Depuy : Arthrodese Lombaire : Cages Concorde

1	Tige d'essai pour cage Concorde Taille 8	DS 2878-04-008
1	Tige d'essai pour cage Concorde Taille 9	DS 2878-04-009
1	Tige d'essai pour cage Concorde Taille 10	DS 2878-04-010
1	Tige d'essai pour cage Concorde Taille 11	DS 2878-04-011
1	Tige d'essai pour cage Concorde Taille 12	DS 2878-04-012
1	Tige d'essai pour cage Concorde Taille 13	DS 2878-04-013
1	Impacteur droit pour cage Concorde	2879-02-000
2	Tiges en baionette d'insertion de cage Concorde ---------→ 2 pièces	2879-01-009



Détail type de set

Curetage H (GYCURTGN#)
Gynecologie

Emballage : One Step KC 390 121 X 121
Type de : Panier DIN 6cm
STU : 0.1333
Salle : L Ultrason + Cycle Lavage Sechage
Utilisation : Réutilisable
Propre : P Stérilisation 134°C Normal

Long

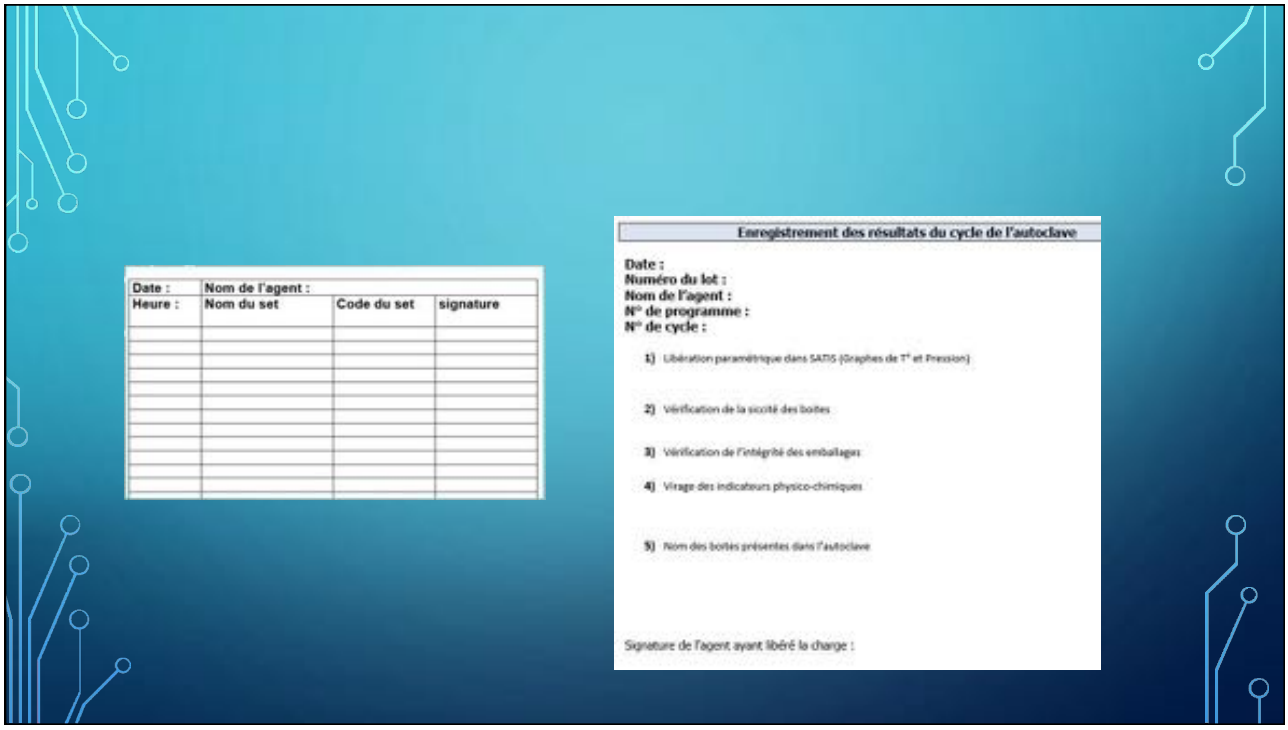
Type Qté. Description

Images type de set

1 1 **Sterili générale Paire de Ciseaux Mayo Courbe 170 mm (18)**
Ref :03.57.17 MEDICON Sterili générale Paire de Ciseaux Mayo Cour
Ref :BC557R AESCULAP Sterili générale Paire de Ciseaux Mayo Cour
Ref :BC587R AESCULAP
Ref :AA 171-17 GEOMED Sterili générale Paire de Ciseaux Mayo Cour
Ref :AA 161-17 GEOMED Sterili générale Paire de Ciseaux Mayo Cour
Ref :835040 LANDANGER Sterili générale Paire de Ciseaux Mayo Cour
Ref :00.501.17 SIMAL Sterili générale Paire de Ciseaux Mayo Cour Ref :11-171-17
MARTIN

1 1 **Sterili générale Paire de Ciseaux Mayo Droit 170mm(18)**
Ref :03.50.17 MEDICON Sterili générale Paire de Ciseaux Mayo Droit
Ref :BC547R AESCULAP
Ref :AA 170-17 GEOMED Sterili générale Ciseaux Mayo Droit 170mm
Ref :AD 510-17 GEOMED
Ref :AA 160-17 GEOMED
Ref :035803 MEDILANE
Ref :11-170-17 MARTIN Sterili générale Paire de Ciseaux Mayo Droit

1 1 **Sterili générale Paire de Ciseaux Mayo Courbe 230 mm (19)**
Ref :03.53.23 MEDICON
Ref :AA 171-23 GEOMED Sterili générale Paire de ciseaux Mayo courb Ref
:00.521.23 SIMAL



Date :	Nom de l'agent :		
Heure :	Nom du set	Code du set	signature

Enregistrement des résultats du cycle de l'autoclave

Date :
Numéro du lot :
Nom de l'agent :
N° de programme :
N° de cycle :

1) Libération paramétrique dans SATIS (Graphes de T° et Pression)
2) Vérification de la siccité des boites
3) Vérification de l'intégrité des emballages
4) Virage des indicateurs physico-chimiques
5) Nom des boites présentes dans l'autoclave

Signature de l'agent ayant libéré la charge :

QU'AVONS-NOUS MIS EN PLACE DEPUIS :

- Multiplication des moyens d'extraction des cycles des machines
- Listings des sets sur papier et clef usb
- Procédure de lecture de cycles papier mise à jour
- Impression directe des derniers cycles de chaque machine (EN COURS)
- Procédure dégradée pour différents types de pannes
- Documents types disponibles dans le bureau répertoriés dans des fardes

POUR LECHWAPI

Réputation atteinte à court terme puisque la majorité des logiciels importants ont été opérationnels dans les 48h.

LESPOINTS POSITIFS AU CHWAPI

- La réactivité des équipes informatiques
- Une prise de conscience immédiate par l'ensemble de l'institution de la gravité de la situation et une participation active au mode dégradé
- Continuité des soins assurée grâce aux documents vierges qui étaient conservés (mais historique patients perdu)

POUR LEFUTUR...

Pour le service informatique :

Surveillance 24h/24 du réseau
Tous les serveurs dédoublés afin de permettre une bascule en moins de 30 minutes

Pour le service de stérilisation :

Listings papiers classés par sets et par disciplines
Transfert des cycles des LD et stérilisateurs via clé USB directement sur l'appareil et impression direct

COMMENT GÉRER UNE ATTAQUE ?

Au niveau informatique :

- Alerter et endiguer
- Comprendre l'attaque
- Durcir et surveiller

Au niveau des services

:

- Mobiliser
- Relancer l'activité
- Maintenir la confiance

Tirer les leçons du vécu

MERCI POUR VOTRE ATTENTION