ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte rendu du Lundi de la cybersécurité du 15 juin 2026

Cyber attaque sur un Centre Hospitalier : Étude de cas et stratégie de mitigation

Présenté par Thomas VADOT et Judith NICOGOSSIAN

Organisé par Pr. Gérard Peliks, Béatrice Laurent et Pr. Ahmed Mehaoua
Rédigé par Rayan Al Mohaize, étudiant en Master 2 Cybersécurité

Table des matières

I Introduction

L'événement « Lundi de la Cybersécurité » est une série mensuelle de conférences en ligne organisée de manière indépendante par Gérard Peliks et Béatrice Laurent. Elle a pour vocation d'explorer chaque mois une thématique différente liée aux enjeux contemporains de la sécurité numérique et de la société.

1 Le thème des Cyber attaques en centre hospitalier

Le Lundi de la cybersécurité du 15 juin 2026 portait sur les Cyber attaques en centre hospitalier. Lors de ce webinaire, Thomas VADOT et Judith NICOGOSSIAN nous ont présenté leur retour d'expérience et leur analyse d'une cyber attaque ayant touché leur établissement de santé, le Centre Hospitalier Intercommunal de Haute-Comté (CHIHC). L'intervention est construite comme une narration "heure par heure" de la crise et de sa gestion : découverte de l'attaque, différents incidents, sidération initiale, organisation de la réponse, fonctionnement en mode dégradé, continuité des soins, communication, reconstruction et enseignements tirés de l'événement.

2 Les intervenants

Pour animer ce Lundi de la cybersécurité, **Thomas VADOT**, RSSI du CHI de Haute-Comté, ainsi que **Judith NICOGOSSIAN**, docteure en anthropologie, spécialisée dans les environnements de santé, nous font l'honneur de nous partager leur expérience lors de la cyber attaque ayant touché leur centre hospitalier.

Par la suite, **Vincent TRELY**, nous a présenté l'APSSIS dont il est le président, pour le "quart d'heure des associations".

II Cyber attaque sur un Centre Hospitalier (Par Thomas VADOT)

1 Le récit

Le récit de Thomas VADOT suit la crise en 6 mouvements :

- Avant l'attaque
- La nuit du 18 au 19 octobre
- Les premières heures
- Le mode dégradé
- La reconstruction
- La transformation

1.1 Avant l'attaque

Thomas VADOT explique qu'avant l'attaque, l'hôpital présentait déjà des fragilités connues : des dettes techniques et financières, des dépendances numériques et des vulnérabilités. L'attaque ne vient pas de nulle part, elle survient dans un système vivant en transformation constante et très exposé.

2 La nuit du 18 au 19 octobre et les premières heures

À ce moment-là, la crise devient réelle et irréversible. Les pannes s'accumulent et deviennent de plus en plus profondes. Il n'est plus possible de compter sur le numérique pour continuer les soins. À ce moment-là, il faut faire preuve de résilience dès les premières minutes, qui sont les plus importantes. L'hôpital n'est pas un centre isolé, généralement les hôpitaux sont tous interconnectés dans une même région et travaillent en collaboration, notamment dans ces moments de crise. Ainsi, Thomas VADOT a pu s'appuyer sur un réseau de CHI pour mener la gestion de crise et gérer les premières minutes.

2.1 Le mode dégradé

Vient ensuite le mode dégradé, nécessaire pour la continuité des soins. Il faut réinventer les circuits, redistribuer les rôles, faire circuler l'information autrement, sachant que le support téléphonique n'est plus disponible, et réutiliser les fax, qui sont des technologies inconnues des jeunes générations. Le but est d'être résilient et de s'adapter au mieux.

2.2 La reconstruction et la transformation

Cette phase permet de rebâtir quelque chose de plus sûr, de plus robuste et de plus maîtrisé. Dans le contexte de cette attaque très poussée et dévastatrice, le but n'est pas d'aller vite pour remettre les applications métier en service, mais de faire table rase et de prendre le temps de tout reconstruire. Pour cela, Thomas VADOT a été accompagné de l'ANSSI et du CERT Santé.

Cette chronologie raconte comment une organisation doit se transformer lorsqu'elle est confrontée à ses propres vulnérabilités. Le but est de transformer l'épreuve en apprentissage, la sidération en méthode et le KO en reconstruction. Cela permet de comprendre les évènements et d'en apprendre sur la résilience hospitalière.

3 La thèse de Thomas VADOT

Cette thèse mobilise une lecture croisée des sciences de gestion, de la résilience et du bricolage organisationnel. La réponse à une attaque ne relève pas d'un protocole technique seul, elle combine ajustements humains, coordination interprofessionnelle et leadership sous incertitude. Elle permet d'étudier la cyber attaque comme une mise à l'épreuve de toute l'organisation et non comme un incident isolé.

Cette thèse est bâtie sur trois leviers :

- La conduite du changement (naviguer sous contrainte)
- Le bricolage organisationnel (faire autrement qu'avant)
- La dynamique de résilience (absorber, adapter, rebondir)

4 L'hôpital avant l'impact

Avant l'incident, plusieurs vulnérabilités étaient connues et exposaient l'hôpital à des risques cyber :

— **Accès distants exposés :** Connexions à distance nécessaires mais dont la sécurisation n'avait pas encore atteint le niveau requis face aux nouvelles menaces.
— **Authentification classique :** Le MFA n'était pas encore universellement déployé, laissant des points d'entrée accessibles à des attaquants déterminés.
— **Segmentation incomplète :** La segmentation réseau était engagée mais pas totalement déployée, rendant possible une propagation latérale en cas de compromission.
— **Supervision cyber immature :** L'absence d'un SOC pleinement opérationnel limitait la détection précoce et l'alerte en temps réel sur les comportements anormaux.

5 2h du matin

Le milieu de la nuit est généralement le moment privilégié pour un attaquant malveillant. À ce moment, il n'y avait que quelques personnes en astreinte, beaucoup de personnes en congé et une équipe IT absente. C'est à ce moment-là qu'une attaque devient dévastatrice et mène au KO. Les premiers signaux de l'attaque apparaissent l'un après l'autre.
— **Chiffrement massif :** Fichiers, dossiers, partages réseau verrouillés un à un dans un silence algorithmique.
— **Applications hors ligne :** Les applications de DPI, de prescriptions et de planification sont inaccessibles. L'hôpital devient aveugle.
— **Téléphonie perturbée :** La coordination interne se fracture. On ne peut plus se parler. On ne peut plus se synchroniser.
— **Message de rançon :** Sur les écrans encore allumés : l'injonction des attaquants. Ce n'est plus une alerte, c'est une déclaration de guerre. le message demande un virement en bitcoin pour obtenir la clé de chiffrement permettant de déchiffrer les données de l'hôpital.

À ce moment-là, il n'y a plus de doute, c'est une cyber attaque, il faut donc agir en conséquence. Les premiers gestes sont les plus importants :
— Arrêt d'internet pour que l'attaquant ne puisse plus avoir la possibilité de piloter à distance
— Isoler le réseau et couper les VPN
— Blocage des interconnexions et interdiction de tout contact vers l'extérieur.
— Conservation des logs pour faire du forensic par la suite.
— Lancement de la cellule de crise

6 La cellule de crise

La cellule de crise s'organise sur trois niveaux :
— **Niveau terrain :** Urgences, bloc, maternité, imagerie, laboratoire. Adaptation clinique immédiate et protocoles dégradés.
— **Niveau opérationnel :** DSI, équipes techniques, référents pôles, pharmacie, logistique. Coordination et remontée terrain en temps réel.
— **Niveau stratégique :** Direction générale, direction médicale, RSSI. Arbitrages de fond, communication externe, décisions engageantes.

7 Le PCA

Le PCA est un travail de mémoire collective pour permettre aux équipes d'agir avec résilience et de manière réfléchie et structurée dans des moments de crise. Ce dernier est constitué des éléments suivants :

- Des fiches réflexes montrant les procédures à suivre en cas d'incidents et permettant à chacun d'agir en autonomie
- Des exercices antérieurs simulant des crises permettant à chacun de savoir ce qu'il a à faire lors d'une crise
- Des supports papiers déjà préparés pour mener à bien le mode dégradé et s'adapter rapidement
- La mise en place d'un langage commun pour agir efficacement

La continuité d'activité est particulièrement importante pour l'hôpital, et il est nécessaire de la mener au mieux. Elle permet avant tout d'assurer la continuité des soins, et pour cela 4 services sont primordiaux :

- **Urgences maintenues :** Aucun patient refusé. Fonctionnement continu avec coordination renforcée SAMU et structures régionales.
- **Bloc et maternité :** Actes urgents maintenus. Coordination orale renforcée entre chirurgiens et anesthésistes, supports papier.
- **Imagerie et laboratoire :** Priorisation des examens critiques. Résultats transmis par fax et téléphone. Aucun résultat vital en suspens.
- **Pharmacie :** Ordonnances manuscrites, circuits papier validés, registres physiques avec double vérification systématique.

8 La remédiation

Cette étape s'est faite en collaboration avec l'ANSSI et le CERT pour rebâtir le SI, cartographier les systèmes plus sensibles et les plus impactés par l'attaque, mener toute la partie investigation, et enfin entamer la partie reconstruction complète du SI.

Avant l'attaque, l'hôpital avait mis en place une feuille de route pour l'amélioration de ses SI comprenant notamment un tiering modèle reposant sur une segmentation stricte des ressources et des comptes, une refonte de l'AD, une revue complète des comptes, etc. Cette feuille de route prévoyait un travail étalé sur trois ans, et tout ce travail a été réalisé lors de cette période de remédiation avec l'ANSSI et le CERT en seulement six mois.

9 Le PRA et la bulle de confiance

Le PRA repose sur un redémarrage minutieux et contrôlé. Il ne faut pas chercher à redémarrer trop vite car cela peut présenter un risque de se faire réattaquer rapidement. Ainsi, un mode de remise en route doit être bien réfléchi et il faut prendre le temps nécessaire pour la reconstruction, en sachant que le personnel a pu s'adapter au mode dégradé.
Thomas VADOT nous présente un plan de reprise d'activité en 4 étapes :

- **La Bulle de confiance :** Environnement réseau isolé, nettoyé, surveillé. Aucun système n'y accède sans validation préalable.
- **Test des sauvegardes :** Sauvegardes secondaires et tertiaires vérifiées, testées en restauration. Seules les sauvegardes certifiées propres entrent dans la bulle.

— **Priorisation clinique :** DPI, pharmacie, urgences, biologie — premiers réintroduits. La priorisation clinique guide l'ordre de reprise technique.
— **Remise en service par paliers :** Chaque service reprend après validation. Montée en charge progressive, surveillée, réversible.

10 PCA versus PRA

Il est important de comprendre la différence entre PCA (plan de continuité d'activité) et PRA (plan de reprise d'activité).

Le PCA est une phase qui se déroule dès les premières heures de la crise et permet de maintenir le bon déroulement des missions avec les moyens dégradés. C'est un plan de nature organisationnelle et la question clé qui se pose dans le cadre de l'attaque du CHIHC est "Comment continuer à soigner les patients ?".

Le PRA se fait après la stabilisation de la situation et lorsque la continuité d'activité a été assurée par les métiers en se réappropriant leurs outils en mode dégradé. La question clé à se poser maintenant est « Comment reconstruire l'outil sans se réinfecter ? ». C'est une étape de nature plus technique et qui nécessite des audits minutieux des systèmes. La cyber attaque touche les SI mais aussi les finances car en mode dégradé il est très compliqué notamment d'assurer les facturations. Ainsi, l'objectif du PRA est aussi d'assurer la reprise financière de l'hôpital, et c'est ce qui rend cette étape encore plus cruciale et complexe.

11 Les facteurs aggravants

Les facteurs aggravants sont principalement ceux qui entraînent un effet domino :
— **Hébergement mutualisé :** Un seul environnement pour plusieurs établissements ; une compromission initiale se propage sans traverser de frontière technique signifiante.
— **Approbations de domaine partagées :** Un Active Directory commun permet à l'attaquant ayant compromis un compte de se mouvoir librement dans l'ensemble du périmètre.
— **Sauvegardes centralisées et accessibles :** Des sauvegardes accessibles depuis le réseau compromis sans isolation ni immuabilité deviennent elles-mêmes des cibles à chiffrer ou détruire.

12 Les facteurs de résilience

La résilience ne s'improvise pas le jour J, elle s'entraîne avant. Ce qui a permis de faire face est le résultat d'une préparation patiente et d'investissements antérieurs.
— **Sauvegardes immuables :** Hors ligne, non altérables, régulièrement testées. La ligne de défense la plus décisive lors de l'attaque.
— **Documentation à jour :** Procédures actualisées, schémas réseau, fiches de contact, un actif stratégique, pas une formalité.
— **Expertise interne :** Double culture technique et clinique déterminante. Elle ne s'acquiert pas dans l'urgence, elle se construit dans la durée.
— **Appui institutionnel :** ANSSI et CERT Santé ; cadre d'action clair, ressources et légitimité. Ces partenariats se nouent avant la crise.

— **Partenaires de confiance :** Prestataires identifiés, contrats actifs, relations préétablies, mobilisation rapide sans les délais d'une mise en relation dans l'urgence
— **Exercices antérieurs :** Les simulations ont forgé des réflexes collectifs. Le sang-froid le jour J est la mémoire musculaire d'une organisation entraînée.

Thomas VADOT souligne que l'attaque a été maîtrisée grâce aux experts métier et technique en interne. Ils se sont vite rendu compte qu'ils ne pouvaient pas s'appuyer sur les éditeurs de logiciels industriels. Pour Thomas VADOT, un industriel doit être en mesure de présenter des mesures de sécurité, un PCA et un PRA à la vente de son logiciel, sinon ce dernier n'a aucune valeur.

13 Ce que la crise a transformé

— **Authentification forte (MFA) :** Déploiement systématique sur l'ensemble des accès critiques. Mesure à fort impact, faible coût, immédiatement généralisable.
— **Segmentation réseau :** Cloisonnement des zones critiques — blocs, laboratoires, pharmacie — avec des règles de flux strictes et auditées.
— **EDR, SOC et SIEM :** Visibilité en temps réel sur les endpoints et les événements de sécurité — un prérequis opérationnel, non une option.
— **Refonte PCA / PRA :** Plans révisés à la lumière de l'expérience vécue. Scénarios réalistes, rôles clarifiés, exercices réguliers intégrés.

14 L'éclairage de Judith Nicogossian

Judith Nicogossian, docteure en anthropologie et spécialiste des dynamiques collectives en situation de crise, nous apporte un éclairage anthropologique sur cette situation.

Le sujet est l'impact de l'attaque sur l'organisation, les services et les personnes. Judith Nicogossian nous parle de la proposition d'un métier transverse ou de formations ayant pour objectifs de prendre en charge la dimension humaine aux côtés des enjeux de la remédiation technique, et de soutenir la gouvernance en étant aux côtés du personnel métier pour leur permettre d'être résilient. L'objectif est d'éviter de céder à la pression, d'éviter d'être submergé par les informations et de pouvoir assurer la communication. Pour cela il est important d'être préparé, d'avoir un plan mis en place par l'organisation et d'être sensibilisé.

Un des effets de ce stress aigu lors d'une situation de crise peut être le burn-out ou la dépression, notamment dans des crises qui durent longtemps telles que celle du CHIHC. Ainsi il est fondamental de préserver les équipes qui sont avant tout des humains.

En situation de crise, les professionnels doivent s'adapter et se retrouvent parfois en dehors des règles et des procédures. Dans le cas de l'attaque du CHIHC, il a fallu reprioriser les missions et les tâches dans certains services et cela peut mener encore une fois à du stress chronique ou à de la culpabilité, ce qui fait du personnel des personnes à risque devant être soutenues dans ces situations. Ce type de risque devient un sujet de plus en plus important dans la médecine du travail, tandis que les cyber attaques ne font que se multiplier, particulièrement en milieu hospitalier.

La crise n'est pas seulement une chaîne de décisions rationnelles. C'est une expérience humaine partagée, traversée par des peurs, des alliances et des gestes de soutien.

Dans une crise cyber hospitalière, l'humain n'est pas un facteur périphérique, il est le cœur battant de la remédiation.

III Présentation de l'APSSIS (Par Vincent TRELY)

L'APSSIS (Association Pour la Sécurité des Systèmes d'Information de Santé) est une association rassemblant environ 1000 personnes et composée de 240 membres pouvant être des institutionnels, des établissements de santé publics et privés, des cabinets d'avocats, des industriels, etc.

L'APSSIS soutient notamment les hôpitaux dans le cadre d'un décret imposant à tout établissement de santé de faire des exercices de cybercrise et de mettre en place des PCA et PRA.

L'APSSIS réunit ses membres tous les ans au congrès national de sécurité des SI de santé du Mans. Près de 220 personnes sont présentes sur 3 jours et 32 conférences y sont organisées.

IV Questions / Réponses

Quelles sont les conséquences de la dépendance à Microsoft ?
Tout dépend de Microsoft, la souveraineté demande beaucoup de travail, des administrations telles que la gendarmerie utilisent Linux pour s'adapter aux problématiques de sécurité. Il est très difficile d'être complètement souverain.

Le papier crayon peut-il fonctionner pour toute activité exposée sur internet ?
Le papier-crayon ne peut pas tout faire, c'est pour cela qu'il est important d'être soutenu par d'autres organismes tels que l'ANSSI et le CERT, d'autres départements de santé, des partenaires tels que des opérateurs pour mettre en place des mini-réseaux avec des box 5G. Tout cela repose sur du bricolage.

Y a-t-il eu d'autres moyens utilisés en dehors des fax lors du passage en mode dégradé ?
Réponse de Khalid SOUMANNE, médecin au CHIHC : WhatsApp a beaucoup été utilisé. Cependant, dans le cadre des soins des patients, il y a des traitements et des données de santé qui sont confidentiels, il fallait donc les utiliser avec beaucoup de rigueur et de précautions.

Côté financier, est-ce que l'ARS a pu se débrouiller autrement ?
Réponse de Khalid SOUMANNE, médecin au CHIHC : L'ARS était présente et a beaucoup aidé. Mais il faut savoir que tous les mois les données de production d'activité sont envoyées à l'ARS, et un arrêté de versement est fait en fonction de cette activité. À ce moment-là, il n'était pas possible d'envoyer ces données. L'ARS a donc forcé les arrêtés de versement en faisant une moyenne de l'année dernière et a versé la somme.

Sauf que l'information n'a pas été bien produite pendant la crise car elle n'a été gérée que par des bouts de papier. Ainsi toutes les informations ne pouvaient pas être transmises ultérieurement à l'ARS, donc il y a eu une perte financière.

Quand le SI a été remis en place, comment les sauvegardes ont elles été récupérées ?
Elles ont été récupérées grâce à la société Data back, une société française ayant les compétences en interne pour pouvoir reconstruire une VM qui était chiffrée. Ainsi, ils ont réussi à remettre en production des VM et des sauvegardes compromises.
Thomas VADOT rappelle qu'il n'a pas pu se reposer sur les éditeurs de leurs logiciels, car ils ne mettent pas en place de solutions de résilience aux cyber attaques dans leurs produits.

Après le dépôt de plainte, est-ce que le parquet cyber a pris en main l'affaire et est-ce que l'attaquant a été identifié ?
Sur chaque VM compromise et sur chaque demande de rançon, il y avait des signatures laissées par l'attaquant montrant qu'il s'agissait d'un groupuscule russe.

Étant donné qu'il n'y a pas eu de paiement de rançons, y a-t-il eu des données qui ont été divulguées ?
Des investigations et des négociations ont été menées par les forces cyber du RAID et de la gendarmerie pour s'assurer qu'aucune donnée n'a été divulguée. Pour le moment, rien n'a été trouvé mais les procédures d'investigation sont encore en cours.

Les patients ont-ils été touchés par cette attaque ?
Le temps est très précieux pour certaines situations telles que des pathologies cardiaques. Malgré certaines situations délicates, le personnel de santé a pu assurer les soins de tous les patients.
Khalid SOUMANNE ajoute que l'impact le plus important pour les patients serait financier, car toutes les communications ont été coupées, et les mutuelles n'étaient plus joignables. Cependant, certaines mutuelles ont des délais de forclusion. Quand les informations de facturation ont été réintégrées aux logiciels après remédiation, le délai de forclusion était passé et donc certains patients ne pouvaient plus être remboursés. Cependant, c'est l'hôpital qui prend en charge ce remboursement, donc ce n'est pas le patient qui est touché, mais la finance de l'hôpital.