Questionnaire Noobo Antoine Gonnet

QUESTION POUR LA VIDÉO 1

Quelle est l'organisation touchée ?

L'organisation touchée par la cyberattaque est le CHSF (Centre hospitalier sud francilien).

Quel est le secteur d'activité de l'organisation ?

L'organisation est principalement dans le domaine hospitalier.

S'agit-il d'une organisation publique ou privée ?

Il s'agit d'une organisation publique.

Qui témoigne, quel est son métier ?

La personne interrogée est Francinne Corgneux, qui est coordinatrice du personnel médical.

S'agit-il plutôt d'une informaticienne ou d'une utilisatrice ?

Francinne semble plutôt être une utilisatrice.

Quels sont les symptômes de départ ?

Les premiers symptômes ont été des écrans qui se sont noircis. Les soignants ont pensé à une panne ou un bug, mais ont vite vu des caractères chiffrés dessus, des textes en anglais. Ils ont alors contacté le service informatique pour constater une cyberattaque.

À quelle date, et quel jour de la semaine commence la cyberattaque ?

Les premiers signes d'une cyberattaque ont été remarqués un samedi, dans la nuit du 20 au 21 août 2022.

Quelle est la mesure d'urgence prise immédiatement au niveau de l'hôpital ?

Les premières mesures d'urgence ont été prises le dimanche, avec le plan blanc qui visait à détourner les urgences arrivant vers les autres hôpitaux (91, 94).

Quelles sont les mesures d'urgence prises au niveau informatique, qui les prend en charge ?

La première cellule d'urgence a été ouverte, et ils ont diffusé l'information le lundi matin en mettant des papiers sous les portes, précisant de ne pas allumer les PC et informant qu'ils avaient été victimes d'une cyberattaque.

Quelles sont les conséquences immédiates de la malveillance ?

Pour les services :

Les services ont été privés quasiment instantanément de tous leurs instruments de travail. Il n'y avait plus de lumière, tout le monde s'est donc comporté de manière très individualiste par manque d'équipement.

Pour les patients :

Les patients ont été redirigés vers d'autres hôpitaux pour les cas les plus graves, ou ont vu leurs opérations reportées ou annulées en raison du manque d'équipement.

Pour les secrétaires médicales des blocs opératoires :

Les secrétaires ont été très sollicitées puisqu'il n'y avait presque plus de moyen de communiquer à l'intérieur de l'hôpital, au point de finir par faire des burn-out dus à la fatigue et au stress.

Quelles données ont été volées ?

Les données volées concernaient tant les patients que les membres du personnel. Ils ont pu prendre toutes les données des employés ainsi que tous les suivis des patients entre leur admission et leurs opérations, les suivis de médicaments, etc.

La demande de rançon

Comment parvient-elle ?

La demande de rançon a été faite via les imprimantes qui étaient censées être désactivées et qui se mirent toutes ensemble à sortir des affiches demandant 10 millions d'euros.

Quelle est la menace des hackers ?

Les hackers ont menacé de publier toutes leurs données si ces derniers ne payaient pas la rançon.

Quel est le type d'attaque ?

Il s'agit d'une attaque de vols de données ainsi que de désactivations de toutes les machines.

Qui sont les hackers ?

Les hackers présumés sont un groupe russe du nom de Lockbytes.

Quel est le montant de la rançon ?

La rançon s'élevait à 10 millions d'euros.

L'hôpital a-t-il payé la rançon ?

L'hôpital a choisi de ne pas payer la rançon.

Les hackers ont-ils mis en action les menaces ?

Après avoir prévenu l'hôpital qu'ils allaient tout publier et après leur avoir laissé un délai, ces derniers ont publié l'intégralité des données sur le dark web.

La cyberattaque a-t-elle soudé les équipes, pourquoi ?

La cyberattaque n'a pas soudé les équipes ; au contraire, tout le monde s'est soucié de son propre service et de sa personne, il n'y avait donc pas d'esprit d'équipe apparu comme lors de la crise du COVID-19.

Quelle est la première tentation des chefs de service ?

Ils ont essayé de ramener leurs ordinateurs personnels et leurs clés USB personnelles au travail pour pallier au manque de ressources.

Qu'est-il arrivé le 4 octobre ?

Les secrétaires étaient très sollicitées, beaucoup ont arrêté et étaient épuisées. Ils ont comptabilisé 15 arrêts le 4 octobre de la part des secrétaires.

Comment retravaille-t-on :

En septembre ?

Le personnel a passé tout le mois de septembre à utiliser du papier et des crayons.

En octobre ?

Pendant le mois d'octobre, ils ont retrouvé quelques outils mais toujours en mode "dégradé".

En novembre ?

À partir du mois de novembre, ils ont pu prendre à nouveau certains patients.

Cette cyberattaque est-elle complètement terminée ?

La cyberattaque a laissé de graves séquelles, à tel point qu'au moment de l'audio, l'hôpital n'a pu reprendre qu'à 80% et toujours en mode dégradé. Elle n'est donc pas encore totalement traitée.

QUESTIONNAIRE 2

L'organisation

Quelle est l'organisation touchée ?

L'organisation touchée par la cyberattaque est Manutan International.

Quel est le secteur d'activité de l'organisation ?

Il s'agit d'une entreprise leader en distribution B to B (business to business).

S'agit-il d'une organisation publique ou privée ?

Il s'agit d'une entreprise privée.

Qui témoigne, quel est son métier ?

La personne qui témoigne est Sylvain Copiaux et occupe le poste de directeur du système d'information.

S'agit-il plutôt d'un informaticien ou d'un utilisateur ?

Il s'agit là d'un informaticien.

La découverte de la malveillance

Quels sont les symptômes de départ ?

Les premiers symptômes ont été une barrière qui ne reconnaissait plus les plaques. Arrivé à l'accueil, des écrans bleus affichaient un message sur tous les postes demandant une rançon pour récupérer les données, sans quoi rien ne fonctionnerait.

Quel jour de la semaine commence la cyberattaque ?

La cyberattaque a eu lieu un dimanche pendant les vacances scolaires.

Qu'avait souscrit Manutan en prévision d'une cyberattaque ?

Manutan avait souscrit à une cyber assurance en cas d'attaque.

Quelle organisation est immédiatement mise en place ?

Une gestion de crise est mise en place, les entreprises reliées à l'assurance entrent en relation avec les attaquants et prennent en charge toutes les actions à réaliser sur site. De plus, une société experte est appelée pour effectuer un audit et mesurer l'ampleur des dégâts.

Quelles sont les conséquences immédiates de la malveillance ?

Pour les services :

Les services se sont retrouvés entièrement arrêtés, incapables de continuer tout travail.

Quelles sont les mesures d'urgence prises au niveau informatique ?

Les premières mesures prises ont été de se couper du réseau pour s'assurer que les attaquants ne se trouvaient plus dans l'entreprise.

Pourquoi les clients de l'entreprise appellent-ils le DSI ?

Les clients prennent connaissance de ce qui s'est passé et essaient d'estimer les dégâts et de savoir si les données ayant fui pourraient les compromettre.

Quelle est la proportion de l'entreprise à l'arrêt ?

Environ 80% des serveurs auraient été corrompus.

Comment l'entreprise continue-t-elle à pouvoir communiquer ?

L'entreprise a eu recours à une plateforme gérée par l'une des entreprises venues les aider, assurant un échange sécurisé.

Les interactions avec les hackers

Quelle est la menace des hackers ?

La menace des hackers était de garder l'entreprise hors d'état de travailler en attendant qu'ils payent.

Quel est le type d'attaque ?

Il s'agit d'une attaque sur le matériel et les serveurs ainsi que d'un vol de données.

Qui sont les hackers ?

Les hackers n'ont pas été révélés mais semblent venir d'Europe de l'Est.

Pourquoi Manutan ne révèle pas le montant de la rançon demandée ?

Ils ne révèlent pas le montant de la rançon afin de ne pas encourager ces pratiques, car les montants demandés pourraient encourager certains à s'y risquer pour l'argent.

Quand et où les hackers ont-ils réussi à s'introduire dans le SI de l'entreprise ?

Les hackers sont entrés 4 semaines avant l'attaque, en janvier.

Quelles sont les données dérobées ?

Ils ont dérobé les données clients ainsi que les données des employés, allant jusqu'à des copies de passeport ou des RIB.

L'entreprise a-t-elle payé la rançon ? Les hackers ont-ils mis en action les menaces ?

L'entreprise n'a pas payé la rançon et les hackers n'ont pas mis en action les menaces, puisque l'entreprise a réussi à restaurer ses serveurs.

La reconstruction

Quelle organisation le service informatique met-elle en place pour restaurer les données ?

Ils font des roulements pour restaurer leurs données. Heureusement, ils effectuaient des sauvegardes tous les jours.

La cyberattaque a-t-elle soudé les équipes ?

La cyberattaque a permis de souder les équipes, car il y avait une vraie compréhension des besoins des autres de repos afin de tourner et de travailler nuit et jour pour réparer les dégâts. Cette crise a donc été bénéfique aux relations entre employés.

Les enseignements de l'attaque

Qu'est-ce qui a été mis en place suite à cette cyberattaque ?

Ils ont mis en place une formation de cybersécurité rapidement appliquée et un test à passer pour rentrer, qu'il faut réussir à 80% sinon il faut le repasser.

Comment fait-on désormais pour se connecter au SI de l'entreprise ?

Que s'est-il passé au mois d'août ?

Il y a eu une autre attaque au mois d'août qui a été contrée en 2 heures grâce aux sauvegardes. L'attaque a été estimée aussi importante que celle de janvier.

Comparaison entre les deux organisations touchées

Quelles sont les différences et/ou similitudes de ces deux attaques concernant :

Aspect	Différent	Similaire	Précisions
la découverte			
Le jour de la semaine choisi pour l'attaque			
la prise en charge			
La proportion de l'organisation touchée			
l'origine des hackers			
le type d'attaque			
Le montant de la rançon demandé			
les menaces en cas de non-paiement			
le paiement de la rançon			
la communication interne			

l'entraide des équipes			
les enseignements suite à l'attaque			

Découverte : similaire : découverte au hasard pendant une période avec peu de monde.

Jour de la semaine : similaire : un jour de week-end pour éviter trop de monde.

Prise en charge : différent : l'hôpital a essayé de se débrouiller par lui-même, alors que Manutan a fait appel à des professionnels en assurant au préalable une sécurité.

Proportion de l'organisation touchée : similaire et différent : similaire car les deux ont été forcés de stopper leurs activités à cause des événements, différents car l'hôpital a mis plus de temps à s'en sortir et traite des patients à risque, donc avait plus de risques de conditions aggravantes.

Origine des hackers : similaire : tous les deux semblent être des groupes venus de Russie (Europe de l'Est).

Type d'attaque : similaire : on a deux vols de données et des actions handicapant les entreprises visant à stopper leurs activités.

Montant de rançon demandé : différent : on ne connaît pas le montant demandé à Manutan.

Menaces en cas de non-paiement : différent : on avait un risque de divulgation pour le cas de l'hôpital contre une menace de conserver les handicaps sur le matériel pour Manutan.

Paiement de la rançon : similaire : on a dans les deux cas refusé de payer la rançon en trouvant des alternatives.

Communication interne : différent : au sein de l'hôpital personne ne s'entraidait et personne n'était au courant de ce qui se passait puisqu'ils n'avaient pas le temps de s'en soucier, contrairement à Manutan qui a mis en place des cellules dans leurs filiales afin de répondre aux questions.

Entraide des équipes : différent : personne ne s'aidait à l'hôpital et tout le monde s'occupait de son service alors qu'ils se sont tous entraînés à Manutan et ont réussi à créer des liens qu'ils ne pensaient pas possibles.

Enseignement suite à l'attaque : différent : certains ne sont pas encore sortis de la crise et n'ont pas encore de leçons à retenir, et Manutan a réussi à mettre en place de nouvelles pratiques pour pallier à d'autres potentielles attaques.