Exploitation de temoignages de deux organisations ayant subi une cyberattaque

Description du thème

|  |  |
| --- | --- |
| **Propriétés** | **Description** |
| **Intitulé long** | Exploitation de 2 témoignages entendus dans l'émission "Les pieds sur terre" sur France Culture sur 2 organisations ayant subi une cyberattaque. |
| **Formation(s) concernée(s)** | BTS Services Informatiques aux Organisations pour les deux options SISR et SLAM. |
| **Matière(s)** | Bloc 3 – Cybersécurité des services informatiques |
| **Présentation** | Deux organisations, l'une publique et l'autre privée ont subi une cyberattaque. Deux personnes racontent ce qui a été vécu de "l'intérieur" et décrivent les différentes étapes qui ont été nécessaires à la remise en état du système d'information. |
| **Savoirs** |  |
| **Compétences** |  |
| **Transversalité** | BTS SIO bloc3, CEJMA |
| **Prérequis** |  |
| **Outils** | Un dispositif permettant de lire un fichier mp3 |
| **Mots-clés** |  |
| **Durée** | 2 heures 30 réparties en 2 séances |
| **Auteur.e(s)** | Hervé L'helguen – Relecture : Valérie Martinez |
| **Version** | v .0 |
| **Date de publication** | Octobre 2023 |

|  |
| --- |
| Pour information, Radio France a donné son accord pour la diffusion en classe du contenu de l'émission fourni au format mp3.  Une image contenant texte, clipart  Description générée automatiquement |

Dernières révisions

Ce tableau contient les modifications apportées au document après sa publication uniquement.

|  |  |  |
| --- | --- | --- |
| **Date** | **Auteur.e** | **Description** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |



A INTRODUCTION

Issu de l'émission de France Culture "Les pieds sur terre" présenté par la journaliste Sonia Kronlund, cet épisode donne la parole à deux personnes de deux organisations ayant subi récemment (en 2022) une cyberattaque.

Il est proposé aux étudiants d'effectuer une écoute active afin de répondre à un questionnaire sur chaque témoignage et à effectuer ensuite une comparaison des deux cyberattaques.

# Matériel fourni

* L'émission au format mp3 :
  + - * Fichier a - Introduction et témoignage n°1 (durée 13:48)
      * Fichier b – Témoignage n°2 (durée 13:00)
* Questionnaire sur le témoignage n°1
* Questionnaire sur le témoignage n°2
* Grille de comparaison des deux cyberattaques

# Scénario

* Semaine 1 (1 heure)
  + Diffusion de l'introduction de la journaliste Sonia Kronlund (**0:00 – 01:30**),
  + Le professeur donne les consignes, à savoir : les étudiants vont devoir prendre des notes au fur et à mesure de l'écoute afin de répondre à un questionnaire qui leur sera fourni juste après l’écoute,
  + Diffusion du témoignage n°1 (**Durée 11:30**),
  + Le professeur distribue le questionnaire n°1,
  + Les étudiants remplissent individuellement le questionnaire,
  + Mise en commun animée par le professeur, l'occasion de répondre complètement au questionnaire, de revoir les concepts associés, de définir le vocabulaire métier, … Il leur est indiqué qu'une autre écoute similaire sera effectuée la semaine suivante, ils pourront alors optimiser leur prise de notes.
* Semaine 2 (1 heure 30)
  + Diffusion du témoignage n°2 (**Durée 13:00**)
  + Le professeur distribue le questionnaire n°2,
  + Les étudiants remplissent individuellement le questionnaire à l'aide de leur écoute et de leurs notes,
  + Mise en commun animée par le professeur.
  + Les étudiants remplissent la grille de comparaison,
  + Mise en commun et conclusion animée par le professeur, ou alors le remplissage et la conclusion sont effectués directement au tableau.

B QUESTIONNAIRE n°1

**L'organisation**

Quelle est l'organisation touchée ?

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

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

Qui témoigne, quel est son métier ?

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

**La découverte de la malveillance**

Quels sont les symptômes de départ ?

A quelle date, et quel jour de la semaine commence la cyber-attaque ?

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

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

**Quelles sont les conséquences immédiates de la malveillance ?**

Pour les services

Pour les patients

Pour les secrétaires médicales des blocs opératoires ?

Quelles données ont été volées ?

**La demande de rançon**

Comment parvient-elle ?

Quelle est la menace des hackers ?

Quel est le type d'attaque ?

Qui sont les hackers?

Quel est le montant de la rançon ?

L'hôpital a-t-il payé la rançon ?

Les hackers ont-ils mis en action les menaces ?

**Travailler en mode dégradé**

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

Quelle est la première tentation des chefs de service ?

Qu'est-il arrivé le 4 octobre ?

**La reconstruction**

Comment retravaille-t-on :

* En septembre ?
* En octobre ?
* En Novembre ?

Cette cyber attaque est-elle complètement terminée ?

B QUESTIONNAIRE n°2

**L'organisation**

Quelle est l'organisation touchée ?

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

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

Qui témoigne, quel est son métier ?

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

**La découverte de la malveillance**

Quels sont les symptômes de départ ?

Quel jour de la semaine commence la cyberattaque ?

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

Quelle organisation est immédiatement mise en place ?

**Quelles sont les conséquences immédiates de la malveillance ?**

Pour les services

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

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

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

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

**Les interactions avec les hackers**

Quelle est la menace des hackers ?

Quel est le type d'attaque ?

Qui sont les hackers?

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

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

Quelles sont les données dérobées ?

L'entreprise a-t-elle payé la rançon ?

Les hackers ont-ils mis en action les menaces ?

**La reconstruction**

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

La cyberattaque a-t-elle soudé les équipes ?

**Les enseignements de l'attaque**

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

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

Que s'est-il passé au mois d'août ?

C GRILLE DE MISE EN COMMUN

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 |  |  |  |

Quelles conclusions peut-on faire de ces deux situations ?