Travaux pratiques – Études de cas relatives à la cybersécurité (version de l'instructeur)

**Remarque à l'intention de l'instructeur**: le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

1. Objectifs

Rechercher et analyser les incidents liés à la cybersécurité

1. Contexte/scénario

Les gouvernements, les entreprises et les particuliers sont de plus en plus ciblés par des cyberattaques. Les experts prédisent d'ailleurs une augmentation du nombre de ces attaques dans les années à venir. La formation à la cybersécurité constitue une priorité internationale, tant les attaques de grande envergure font désormais craindre pour la sécurité de l'économie mondiale. Le CSIS (Center for Strategic and International Studies) estime que la cybercriminalité coûte plus de 400 milliards de dollars à l'économie mondiale chaque année. En outre, 3 000 entreprises ont été victimes d'attaques en 2013 aux États-Unis. Au cours de ces travaux pratiques, vous allez étudier quatre attaques de haut niveau et décrire les différents aspects de chaque attaque (qui, quoi, pourquoi et comment).

1. Ressources requises

* Ordinateur personnel ou terminal mobile avec accès Internet
  1. Effectuez des recherches sur les cyberattaques de haut niveau.
     1. À l'aide de votre moteur de recherche favori, recherchez des informations concernant chacune des cyberattaques listées ci-dessous. Vous obtiendrez sûrement de nombreux résultats allant d'articles de presse à des articles plus techniques.

Faille de sécurité chez Home Depot

Faille ciblant les cartes bancaires Target

Virus Stuxnet

Attaque de Sony Pictures Entertainment

**Remarque** : vous pouvez utiliser le navigateur de la machine virtuelle installée lors d'un TP précédent pour lancer votre recherche sur l'attaque. En utilisant la machine virtuelle, vous évitez d'infecter votre ordinateur avec des malwares.

* + 1. Lisez les articles obtenus à l'étape 1a et préparez une présentation des différents aspects de chaque attaque (qui, quoi, quand, où et pourquoi).
  1. Faites l'analyse à l'écrit d'une cyberattaque.

Sélectionnez l'une des cyberattaques de haut niveau mentionnées à l'étape 1a et rédigez son analyse en répondant aux questions ci-dessous.

1. Qui étaient les victimes de l'attaque ?

**Les victimes de l'attaque étaient Sony Pictures Entertainment, une grande entreprise de divertissement.**

Les réponses varient selon la cyberattaque choisie.

1. Quels outils et technologies ont-ils été utilisés lors de l'attaque ?

**Les attaquants ont utilisé des techniques de phishing avancées, des logiciels malveillants personnalisés et ont exploité des vulnérabilités dans les systèmes de sécurité de Sony.**

Les réponses varient selon la cyberattaque choisie.

1. Quand l'attaque a-t-elle eu lieu sur le réseau ?

**L'attaque a eu lieu en novembre 2014.**

Les réponses varient selon la cyberattaque choisie.

1. Quels systèmes ont-ils été ciblés ?

**Les systèmes informatiques de Sony Pictures Entertainment ont été principalement ciblés, y compris les serveurs, les postes de travail et les bases de données.**

Les réponses varient selon la cyberattaque choisie.

1. Quel était le mobile des hackers au cours de cette attaque ? Quel était leur but ?

**Le groupe de hackers, qui se faisait appeler les Guardians of Peace (GOP), a affirmé que leur mobile était de protester contre la sortie d'un film spécifique et d'exposer les pratiques commerciales de Sony Pictures Entertainment.**

Les réponses varient selon la cyberattaque choisie.

1. Quelles ont été les conséquences de l'attaque ? (données volées, rançon, systèmes endommagés, etc.)

**Les conséquences comprenaient le vol massif de données confidentielles, la divulgation d'emails internes sensibles, des coûts importants liés à la récupération et à la sécurité, et une perturbation significative des opérations commerciales de Sony Pictures Entertainment.**

Les réponses varient selon la cyberattaque choisie.