César SAVIC
BTS SIO1-Grp2
Bloc 3-Cybersécurité

Le:18/09/2023

TD N°1:Sécurité Informatique et Cybercriminalité

Question 1 :

1-Phishing:

Le Phishing est le fait d'envoyer des mails en se faisant passer pour un organisme tels qu'une banque ou autre et de faire un faux mail demandant de mettre à jour vos données personnel sur leurs sites afin de récupérer des données tels que vos numéros de carte bancaires ou vos codes d'accès à certaines entreprise si vous êtes un employé.

La société VosReves est sensible à ce genre d'attaques car leurs employés ont des données privées tels que des codes d'accès au système de l'entreprise.

2-Le DDOS:

Le DDOS ou déni de service distribué est un type d'attaque qui consiste à envoyer un nombre conséquent de requête sur un site web afin que celui-ci se retrouve dans l'incapacité de les gérer et arrête de fonctionner.

La société VosReves est sensible à ce genre d'attaques car tout site web est susceptible de subir une attaque DDOS.

3-Ransomware:

Le ransomware est un type de fonctionnement d'attaque dont la plus commune est l'installation d'un logiciel malveillant qui crypte les données

d’un ordinateur et demande une somme d’argent afin d’y récupérer l’accès grâce à une clé de décryptage que l’attaquant possède.

La société VosReves est susceptible de subir ce genre d’attaques car ce genre de logiciel peut arriver par pièce jointe d’un mail ou avec l’utilisation d’une clé USB inconnue. Des employés non informées à ce genre d’attaques peuvent facilement se faire avoir.

4-Cyberharcèlement:

Le Cyberharcèlement est une type d’attaque centré sur une personne en particulier, celui-ci fonctionne comme le harcèlement normal mais celle-ci fonctionne plus autour de la violence verbale, l’acharnement et les menaces.

La société VosReves n’est pas réellement sensible à ce genre d’attaques étant donné qu’il ne s’agit pas d’une personne cependant les employés eux peuvent en être la victime cependant il a peu de chance que cela affecte l’entreprise.

5-Usurpation d’identité:

L’Usurpation d’identité est une attaque qui consiste à récupérer des données personnelles en amont sur une personne en particulier pour ensuite se faire passer pour cette personne afin d’attaquer les connaissances de cette personne. Ce type d’attaque peut avoir plusieurs buts tels que récupérer des données personnelles sur un grand nombre de personnes ou encore voler de l’argent ou bien même.

La Société VosReves est sensible à ce genre d’attaque car les employés non informés peuvent être du genre a donner beaucoup d’informations sur eux-mêmes sur internet et il peut donc être facile d’usurper l’identité et de voler des données privées de l’entreprise.

6-Spyware:

Le Spyware est un type de logiciel malveillant qui a pour but d’espionner les activités sur un ordinateur en particulier ou sur tout un réseau. Il s’installe de la même manière qu’un ransomware c’est à dire au travers

d’un mail malveillant ou encore l’installation d’un logiciel non officiel ou l’utilisation d’une clé USB inconnue.

La Société VosReves est sensible à ce genre d’attaques car les employés ne font pas forcément attention aux mails qu’ils reçoivent. Et qui peut se faire voler des données importantes avec la surveillance du spyware.

7-Cheval de troie:

Le Cheval de Troie est un type d’attaque qui a pour but d’installer un logiciel malveillant sur un ordinateur les cheval de troie les plus répandu sont ceux installant des logiciels qui ont pour but de prendre le contrôle d’un ordinateur en prenant le contrôle de celui-ci ils peuvent alors faire ce qu’ils veulent et ont accès à toute les données de l’ordinateur en question.

La société VosReves est sensible à ce genre d’attaques car celle-ci fonctionne de la même façon que le spyware et le ransomware à travers de faux mail ou de liens frauduleux. Et les employés qui ne sont pas prudents peuvent facilement se faire avoir par ce genre d’attaques.

8-Fraude à la carte bancaire:

Ce type d’attaque vise à détourner l’argent de quelqu’un à travers un faux site web marchand ce qui mène la victime si elle ne fait pas attention a donnée ses données de carte bancaire sur des sites malveillants et à se faire voler son argent.

La société VosReves n’est pas sensible à ce genre d’attaques mais les employés le sont cependant cela n’aura pas de conséquence pour la société.

9- Chantages à la webcam:

Ce type d’attaques est un type d’attaque qui consiste à récupérer l’accès à la caméra d’une victime ou à prétendre y avoir accès, ce genre d’attaque a pour but de menacer de divulguer des images de la victime dans des moments embarrassants ou autre dans le but de lui faire payer une rançon pour ne pas que les images soit partagés sur internet.

La société VosReves n’est pas sensible à ce genre d’attaques car les employés ne possèdent normalement pas de caméras sur leur poste de travail.

Question 2 :

Type d’attaques	Précautions	Méthodes de protections adéquates
Phishing	Ne pas cliquer sur les pièces jointes des mails suspects. Vérifier les adresses mails	Utiliser le classement automatique des spams mais cette méthode n’est pas infaillible.
DDOS	Avoir plusieurs serveurs afin de ne pas être totalement arrêté lors d’attaques	Mettre en place une architecture complexe, robuste et extensible pour les serveurs.
Ransomware	Effectuer des sauvegardes régulières de ses données,mettre à jour régulièrement ses équipements, faire attentions à certains types d’extensions pour les documents reçus.	Utilisation de sites web qui vérifient les fichiers avant de les installer(Virus Total).
CyberHarcèlement	Ne pas divulguer ses données personnelles sur internet, sécuriser ses mots de passe, faire attention à son image sur internet.	Rester anonyme sur les réseaux sociaux,si des données personnelles sont présentes sur internet il y a la possibilité de les supprimer en faisant une demande au site concerné.
Usurpation d’identité	Ne pas divulguer ses données personnelles sur internet, sécuriser ses mots de passe, faire attention à son image sur internet.	Rester anonyme sur les réseaux sociaux,utiliser des mots de passe complexes.

Spyware	ne pas télécharger d'applications en dehors des boutiques reconnues, mettre à jour régulièrement ses appareils, également faire attention aux pièces jointes dans les mails.	Utilisation de sites web qui vérifient les fichiers avant de les installer(Virus Total). Le classement automatique des spams.
Cheval de Troie	Ne pas cliquer sur les pièces jointes des mails suspects. Effectuer des sauvegardes régulières de ses données,mettre à jour régulièrement ses équipements.	Utilisation de sites web qui vérifient les fichiers avant de les installer(Virus Total). Utiliser le classement automatique des spams.
Fraude à la carte bancaire	ne pas communiquer ses coordonnées bancaires sur des sites web non reconnus. vérifier les mails reçus par sa banque.	Consulter régulièrement les consignes de sécurité de sa banque, choisir un mot de passe sécurisé pour accéder à ses comptes.
Chantage à la webcam	Ne pas cliquer sur les pièces jointes des mails suspects. Effectuer des sauvegardes régulières de ses données,mettre à jour régulièrement ses équipements.	Ne pas acheter de webcams, mettre un cache sur sa webcam quand elle n'est pas utilisée.

Question 3:

1-Formation en ligne :

Proposer des cours de formation en ligne sur des sujets tels que la gestion des mots de passe, la détection de phishing, la navigation sécurisée sur Internet.

2-Ateliers et formations en personne :

Organiser des ateliers et des sessions de formation en personne animés par des experts en sécurité informatique. Ces formations peuvent être plus interactives et adaptées aux besoins de l'organisation.

3-Simulations de phishing :

Mettre en place des campagnes de simulation de phishing pour tester la capacité des employés à repérer les e-mails malveillants.

4-Communication régulière :

Communiquer régulièrement sur les menaces actuelles et les meilleures pratiques de sécurité à l'aide de réunions d'équipe ou de canaux de communication internes.

5-Tests de compétence :

Évaluer régulièrement les compétences en sécurité informatique des employés à l'aide de tests et d'évaluations. Cela peut aider à identifier les lacunes et à cibler davantage la formation.