TAMDA Zohir
BTS SIO 1
Bloc 3 - Cybersécurité

Le 23 septembre 2023

Les types d’attaques

Sommaire

Problématique

Sur Internet, il y a de multitudes d’appareils, indispensables à nos besoins dans la vie quotidienne tels que les téléphones portables, les ordinateurs, les tablettes, les serveurs, les IOT (objets connectés) etc... Or, le réseau a des limites, en effet, des individus mal intentionnés peuvent attaquer le réseau de tout type, à savoir le réseau informatique d’une entreprise, le réseau de la maison, le réseau de la banque etc... Ce qui peut être conséquent suivant la gravité de la situation et de la vraisemblance.

Les types d’attaques

Sur Internet, il y a plusieurs types d’attaques réalisées par des attaquants (ou des hackers) qui font que l’activité d’une organisation (entreprises, associations, banques…) ou d’un individu peuvent être perturbé, que la sécurité informatique n'est pas en point voire pire que les données personnelles/sensibles soient volées. Pour comprendre ces types d’attaques, il faut prendre en compte son fonctionnement, son but et ainsi imaginer le scénario; prenons l’exemple de la société nommée “VosRêves” qui fournissent des voyages pour des clients. Dans ce cas, les 10 types d’attaques connues sont représentées sous forme de tableau.

Type d’attaque	*Fonctionnement*	*Objectif*	*Société VosRêves*
Phishing	Envoyer des faux messages (mails/SMS) aux clients	Faire croire aux clients qu’il s’agit d’un message provenant d’une entreprise alors qu’il ne l’est pas	Pour cette société, il s’agit d’une menace car il y a probablement le vol d’informations. Ils peuvent même avoir plusieurs informations personnelles identiques.
Usurpation d’identité	Se faire prendre pour une autre personne.		Oui parce que la société peut avoir des faux clients.
XSS	Faille consistant à injecter un code qui peut provoquer des erreurs inattendu au niveau de la gestion des données	Manipuler les donnée s dans le serveur	Oui parce que le site de la société peut avoir des failles de sécurité s’il n’est pas patché/corrigé.
Cyberharcèlement	Critiquer/Moquer les victimes sur Internet (dont les réseaux sociaux)		Non car il n’y a rarement (voir pas du tout du harcèlement) sur le site de la société, il est fait pour la réservation des voyages.

Virus	Consiste à faire planter des processus dans un OS.	Rendre l'appareil (quasi) inutilisable	Oui car le virus peut affecter les données s'il est présent sur les serveurs de la BDD.
Ransomware	Logiciel qui crypte automatiquement les données et rend l'appareil inutilisable.	Forcer l'utilisateur à payer une rançon pour récupérer ses données.	Oui car cela peut crypter les données des clients et il sera impossible de le décrypter.
Trojan	Consiste à accéder aux données de l'appareil, voir la contrôler.	Rendre l'appareil (quasi) inutilisable.	Oui car avec le Trojan, il peut affecter/endommager/effacer les données des clients
Spyware	Espionner l'activité de l'ordinateur d'une personne.	Savoir ce que la personne fait sur l'appareil.	Oui car l'attaquant peut récupérer les données du client même avant de soumettre le formulaire.
Spam	Recevoir les messages (mails/SMS) provenant de tous les appareils	Solliciter les personnes à consulter les boîtes mails malveillantes.	Oui car plusieurs messages identiques contiennent des pièces jointes qui peuvent être malveillantes.
DDoS	Consiste à envoyer des requêtes depuis plusieurs ordis	Rendre le serveur inaccessible pour les salariés/clients.	Oui car comme le site de la société a une adresse IP publique, les attaquants pourront faire beaucoup de requêtes surchargées avec plusieurs machines, ce qui rendra ce site inaccessible.

Précautions

Pour faire face à ces types d'attaques, des mesures doivent être prises en suivant les précautions ainsi que des procédures qui sont également représentées sous forme de tableau.

Type d'attaque	***Précautions***	***Méthodes de protection adéquates***
Phishing	Identifier si le message est officiel ou non	Vérifier si le lien est le vrai.
Usurpation d'identité	Contrôler l'identité de la personne.	Utiliser un mot de passe complexe, différent pour chaque compte.
XSS	Patcher le code du site	En utilisant la fonction `htmlentities()` dans PHP (utile pour le serveur web)
Cyberharcèlement	Intervenir, parler envers l'adulte.	Envers les responsables de l'école/police/gendarmerie
Virus	Sécuriser l'ordinateur	Mettre en place un antivirus
Ransomware	Porter plainte.	Envers la gendarmerie/police.
Trojan	Sécuriser l'ordinateur.	Mettre en place un antivirus et un pare-feu.
Spyware		
Spam	Filtrer les spams.	Aller dans les paramètres (Gmail par exemple) et ajouter des adresses mail dans la blacklist.
DDoS	Éviter la réception des requêtes surchargées.	Utiliser une IP dynamique. Mettre en place un pare-feu.

Sensibilisation

Pour sensibiliser les employés d'une entreprise qui peuvent être victimes d'une ou plusieurs types d'attaques. L'entreprise met en place une charte informatique visant à ce que l'on doit faire et à ne pas faire dans un parc informatique *(par exemple : il ne faut pas donner la session à un autre employé. Toujours fermer la session lorsqu'on a terminé de travailler. Ne pas installer des logiciels qui ne sont pas utiles pour l'entreprise ou sans accord)*

Il est également nécessaire de suivre les nouveautés de la loi RGPD car elle permet d'être au courant des nouveaux ajouts dans cette loi et ainsi avoir de meilleurs conseils pour protéger ses données personnelles.