BALDA Nilda, **DEHU Thibault,** **BERNARD Kervin** **BTS SIO1 GP1**	***BLOC 3 - Cybersécurité des systèmes informatique***	**Date : 15/09/2023**

TD1 - Sécurité informatique et cybercriminalité

Partie

Q1. Les différents types d'attaques existantes du système d'Information et en quoi elles peuvent concerner la société VosRêves :..... 3

Q2. les précautions à prendre pour limiter ces risques et rechercher des méthodes de protection adéquates :.....4

Q3. Comment l'entreprise pourrait former les employés à ces méthodes de protection :..... 5

Q1. Les différents types d'attaques existantes du système d'Information et en quoi elles peuvent concerner la société VosRêves :

Types d'attaque /Risque	Fonctionnement	Objectif	Société VosRêves
Phishing	Distribution de faux courriers électronique	Vol de données personnelles	Vulnérable pour les commerciaux
Logiciel malveillant	Création d'un faux site internet ou logiciel comprenant un virus	Récupération de données personnelles de l'ordinateur	Vulnérable pour les employés de bureau
Piratage de mot de passe	Utilisation de tout mot de passe possible, et des recherches approfondies sur les réseaux sociaux.	Vol de compte, récupération des données personnels	Vulnérable
Piratage de site marchand	Création d'un faux site marchand	Récupérer des coordonnées bancaire	Vulnérable pour le secteur finance
Brute Force (Attaque par force brute)	Essayage de toutes combinaisons de mot de passe	Récupération des données personnelles.	Vulnérable pour les employés de bureau
DDOS (Distributed Denial of Service)	Empêcher le fonctionnement d'un site web	C'est de faire un site web inaccessible.	Vulnérable pour les techniciens informatiques
Doxing (Divulgation de données	C'est d'identifier quelqu'un qui est en ligne.	récupérer ses données personnelles.	Vulnérable

personnelles)			
InjectionSQL	Injection de code SQL dans un site ou application WEB	Manipuler une base de données et récupérer des informations	Vulnérable pour les données de l'entreprise
MitM (Man in the Middle)	Les données passent d'abord par le MitM puis au destinataire.	Espionnage et récupération des données.	Vulnérable

Q2. les précautions à prendre pour limiter ces risques et rechercher des méthodes de protection adéquates :

Types d'attaque /Risque	Précautions	Méthodes de protection adéquates
Phishing	Supprimez les emails suspects et ne pas cliquer sur les pièce jointe d'adresse inconnu	Utilisation de logiciel anti-spam **(Avast One)**
Logiciel malveillant	Vérifier que l'adresse HTTP possède un "S"	Antivirus Windows Defender **(Vérification de Tous les Logicielles)**
Piratage de mot de passe	Éviter D'utiliser des Mot de Passe en lien avec vos information personnelles **(Nom,Date de Naissance)**	Authentification A Deux Facteur **(2FA)** avec Google Authentification
Piratage de site marchand	Vérifier que l'adresse HTTP possède un "S", donc soit sécurisé	Utilisation de WOT (Extension pour tester la fiabilité des sites internet)
Brute Force	Posséder un mot de passe forts (Majuscule, chiffres, caractères spéciaux)	Utiliser l'A2F,Google Authentification et changer son mot de passe

DDOS	Avoir un tableau de bord afin de gérer l'attaque	Mise en place du VAC (protection anti-DDoS) afin de stopper l'attaque
Doxing	Limiter la divulgation de ses données Vous pouvez ajouter des titres (Format > Styles de paragraphe) qui apparaîtront dans votre table des matières. personnelles sur internet et rester anonyme	Changez les mots de passes et recueillir des preuves
InjectionSQL	fais en sort que la sécurité est à jour	Validez et filtrez les données d'entrée, effectuez des tests de sécurité
MitM	Éviter d'utiliser des Wi-Fi Public non sécurisé et site web	Faire un test d'intrusion pour voir si il n' y-a pas un intrusion

Q3. Comment l'entreprise pourrait former les employés à ces méthodes de protection :

L'entreprise pourrait utiliser les cours de l'ANSSI afin de former les employés aux risques numériques et d'apprendre à se protéger.

Elle peut aussi réaliser une charte informatique, des sessions de live-hacking (mise en situation d'un piratage) ou encore des sessions d'e-learning, pour former chaque salarié à son rythme.