DEFINITIONS

1. Panorama de la SSI (Sécurité des Systèmes d'Information)

- Cybersécurité: Ensemble des moyens mis en œuvre pour protéger les systèmes informatiques, réseaux, et données contre les menaces et les attaques informatiques.

Attaque informatique: Action visant à compromettre la confidentialité, l'intégrité, ou la disponibilité des informations d'un système informatique. –

Cyberespace: Environnement virtuel où se déroulent les activités liées à Internet, incluant les réseaux, les serveurs, et les données.

Infrastructure critique: Systèmes essentiels à la sécurité nationale, tels que l'énergie, les télécommunications, les transports, susceptibles d'être ciblés par des attaques.

2. Sécurité de l'Authentification

Authentification: Processus permettant de vérifier l'identité d'un utilisateur ou d'un système, généralement par l'utilisation de mots de passe, de clés, ou de dispositifs biométriques.

Attaque par force brute: Méthode où un attaquant essaie de déchiffrer un mot de passe en essayant toutes les combinaisons possibles jusqu'à trouver la bonne.

Cryptographie: Science des codes secrets, utilisée en sécurité informatique pour protéger les données par des méthodes de chiffrement et de déchiffrement.

3. Sécurité sur Internet

Firewall: Dispositif de sécurité réseau qui contrôle le flux du trafic, autorisant ou bloquant les communications en fonction de règles prédéfinies.

Phishing: Technique d'attaque où des informations personnelles sont obtenues en se faisant passer pour une entité de confiance.

VPN (Réseau Privé Virtuel): Technologie permettant de créer une connexion sécurisée sur Internet, assurant la confidentialité des données échangées.

4. Sécurité du Poste de Travail et Nomadisme

Antivirus: Logiciel conçu pour détecter, prévenir, et éliminer les programmes malveillants, tels que les virus et les logiciels espions.

BYOD (Bring Your Own Device): Politique permettant aux employés d'utiliser leurs propres appareils (ordinateurs, smartphones) au travail, nécessitant des mesures de sécurité spécifiques. –

Authentification à deux facteurs (2FA): Méthode de sécurité où l'accès à un système nécessite deux formes d'identification distinctes, augmentant la sécurité du processus