Définitions CyberSécurité

Internet : Réseau mondial interconnecté permettant la communication et l'échange d'informations à l'échelle planétaire.

Client : Un dispositif ou programme informatique qui demande des services ou des ressources à un serveur.

Serveur : Un ordinateur ou un programme qui fournit des services, des ressources ou des données à d'autres ordinateurs, appelés clients, dans un réseau.

Cybersécurité : Ensemble des mesures visant à protéger les systèmes informatiques, les réseaux et les données contre les attaques, les dommages ou l'accès non autorisé.

Malware : Terme générique désignant les logiciels malveillants, tels que les virus, les vers, les chevaux de Troie, conçus pour causer des dommages à un ordinateur, un réseau ou un utilisateur.

Spam : Envoi massif et non sollicité de messages électroniques, souvent à des fins publicitaires.

BotNet : Réseau de dispositifs informatiques infectés par des logiciels malveillants et contrôlés à distance par un attaquant, souvent utilisé pour des activités illégales.

Rançongiciel : Logiciel malveillant qui chiffre les fichiers d'un utilisateur et demande une rançon en échange de leur déchiffrement.

Typosquatting : Pratique consistant à enregistrer des noms de domaine similaires à des noms populaires dans l'espoir de capturer du trafic Web destiné à ces sites populaires.

SMTP (Simple Mail Transfer Protocol) : Protocole de communication utilisé pour le transfert de courriers électroniques.

IP (Internet Protocol) : Protocole réseau qui attribue des adresses uniques aux appareils connectés à Internet.

Serveur Mandataire (Proxy) : Serveur intermédiaire entre un client et un serveur de destination, utilisé pour améliorer la sécurité et la performance.

DNS (Domain Name System) : Système de noms de domaine utilisé pour traduire les noms de domaine en adresses IP.

Cryptographie : Science et art de protéger l'information en la transformant (chiffrage) de manière à la rendre illisible sans la connaissance d'une clé de déchiffrement.

Routeur : Dispositif réseau permettant de diriger le trafic entre différents réseaux.

Firewall : Dispositif de sécurité réseau qui surveille et filtre le trafic entrant et sortant en fonction de règles définies.

Whitehat : Professionnel de la sécurité informatique travaillant de manière éthique pour protéger les systèmes.

Greyhat : Personne qui agit de manière éthiquement ambiguë en matière de sécurité informatique.

Blackhat : Personne utilisant des compétences en sécurité informatique de manière malveillante.

Antivirus : Programme conçu pour détecter, prévenir et éliminer les logiciels malveillants.

Plugins : Modules d'extension ajoutant des fonctionnalités à un logiciel ou un navigateur.

Système d'exploitation : Logiciel qui gère les ressources matérielles d'un ordinateur et fournit une interface pour les applications.

Navigateur web : Application permettant de visualiser des pages web.

Cookie : Petit fichier texte stocké sur l'ordinateur d'un utilisateur par un site web pour stocker des informations sur l'utilisateur.

Le chiffrement : Processus de conversion de données en un format illisible sans la clé de déchiffrement correspondante.

Antimalware : Logiciel conçu pour prévenir, détecter et éliminer les logiciels malveillants.

Périphérique de stockage amovible : Dispositif permettant de stocker des données et pouvant être connecté et déconnecté d'un ordinateur, comme une clé USB.

Clé USB : Petit périphérique de stockage amovible utilisé pour transférer des données entre des ordinateurs.

Séparation des usagers et usages : Pratique visant à délimiter et isoler les utilisations et les utilisateurs sur un système informatique.

Charte informatique : Document définissant les règles et les obligations liées à l'utilisation des technologies de l'information dans un environnement professionnel.

BYOD (Bring Your Own Device) : Pratique permettant aux employés d'utiliser leurs propres dispositifs électroniques au travail.

TCP/IP (Transmission Control Protocol/Internet Protocol) : Ensemble de protocoles de communication utilisés pour interconnecter des dispositifs sur un réseau, notamment sur Internet. TCP/IP définit comment les données sont transmises, reçues et routées entre les ordinateurs.

Cryptage (ou chiffrement) : Il s'agit du processus de conversion de données en un format illisible, généralement dans le but de garantir la confidentialité lors de la transmission ou du stockage des données.

Bruteforce : Une attaque bruteforce est une méthode où un attaquant essaie systématiquement toutes les combinaisons possibles de mots de passe jusqu'à ce qu'il trouve le bon.

Ingénierie sociale : C'est une technique utilisée par les attaquants pour manipuler les individus de manière à obtenir des informations confidentielles, telles que des mots de passe ou des informations d'identification, en exploitant la confiance ou la crédulité des personnes.

Protocole d'authentification : Il s'agit d'un ensemble de règles et de procédures qui permettent de vérifier l'identité d'une entité, telle qu'un utilisateur ou un système, lors de l'accès à un réseau ou à des données.

Hachage : Une fonction de hachage transforme des données en une chaîne de caractères fixe, souvent sous forme de code hexadécimal. Elle est utilisée pour vérifier l'intégrité des données, mais elle n'est pas réversible.

Gestionnaire de mot de passe : Un outil qui stocke de manière sécurisée les mots de passe et les identifiants, souvent avec la possibilité de les générer de manière aléatoire.

Signature électronique : Une signature électronique est une technique visant à authentifier la provenance et l'intégrité d'un message, d'un document ou d'une transaction électronique.

Chiffrement asymétrique : Un système de chiffrement qui utilise une paire de clés, l'une pour le chiffrement et l'autre pour le déchiffrement.

Chiffrement symétrique : Un système de chiffrement où une seule clé est utilisée pour à la fois le chiffrement et le déchiffrement.

Chiffrement hybride : Une combinaison de chiffrement symétrique et asymétrique, généralement utilisée pour garantir l'efficacité et la sécurité.

Attaque par déni de service (DDoS) : Une attaque visant à rendre un service indisponible en submergeant délibérément le serveur cible avec un trafic excessif.
Attaque de l'homme du milieu : Une attaque où un attaquant intercepte et manipule la communication entre deux parties sans qu'elles en soient conscientes.

Identification biométrique : L'utilisation de caractéristiques physiques ou comportementales uniques, telles que les empreintes digitales ou la reconnaissance faciale, pour identifier et authentifier des individus.

Système d'authentification à double facteur (2FA) : Un mécanisme qui exige deux méthodes distinctes d'authentification avant d'accorder l'accès, par exemple, un mot de passe et un code généré sur un appareil mobile.

Politique de sécurité : Un ensemble de règles et de procédures définissant les pratiques de sécurité d'une organisation.

OIV Cybersécurité : Les Opérateurs d'Importance Vitale (OIV) sont des entités critiques pour le fonctionnement d'un pays, et la cybersécurité des OIV concerne la protection de ces entités contre les cybermenaces.

OCLCTIC : L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication, est un service de police français spécialisé dans la lutte contre la cybercriminalité.