WISER
Wide-Impact cyber SEcurity Risk framework

Glossaire de Cybersécurité pour les novices

Selon des recherches du gouvernement britannique, 74% des petites entreprises au Royaume-Uni ont connu une brèche de cyber-sécurité l'année dernière, et 90% des grandes entreprises ont également été ciblées. Certains incidents ont causé des millions de dommages.

Ce guide s'adresse aux PME et aux petites équipes informatiques des administrations publiques pour comprendre les risques cyber majeurs et apprendre à les gérer efficacement.

Cyber attack (attaque cyber) – Exploitation volontaire de systèmes informatiques, d'entreprises dépendantes du numérique et de réseaux dans l'objectif de nuire.

Cyber incident (incident cyber) –Un événement qui menace réellement ou potentiellement un ordinateur, un périphérique connecté à Internet ou un réseau, ou des données traitées, stockées ou transmises sur ces systèmes, ce qui peut nécessiter une action de réponse pour limiter les conséquences.

Cyber résilience - capacité globale des systèmes d'information et des organisations à résister à des cyber évènements et, se rétablir d'un dommage éventuel.

Cyber sécurité - protection des systèmes connectés à Internet, comprenant le matériel, les logiciels et les infrastructures associées, les données et les services qu'ils fournissent, contre tout accès non autorisé, tout dommage ou tout usage abusif. Cela inclut les dommages causés intentionnellement par l'opérateur du système ou accidentellement, en raison du non suivi des procédures de sécurité volontaire ou à la suite d'une manipulation.

Évaluation des risques liés à la cybersécurité - identifie les faiblesses dans les zones à risque de votre organisation et détermine les actions à mener pour les combler. Il garantit également que vous investissez du temps et de l'argent sur les bons sujets afin de ne gaspillez pas les ressources.

Cyber-menace - tout ce qui peut compromettre la sécurité des systèmes d'information et les dispositifs connectés à Internet, y compris le matériel, les logiciels et l'infrastructure connexe, les données et les services qu'ils fournissent, principalement par des moyens informatiques.

Types d'attaques et de vulnérabilités

Commodity malware – Malware qui est largement disponible à l'achat, ou en téléchargement gratuit, qui n'est pas personnalisé et est utilisé par un large éventail de source de menace.

Data breach (Fuite de données) – diffusion illégitime d'information sur un réseau ou à un tiers qui n'est pas autorisé à y accéder.

DDoS – Les attaques par déni de service se caractérisent par une tentative explicite des attaquants d'empêcher les utilisateurs légitimes d'un service d'utiliser ce service. Dans une attaque de déni de service distribuée (DDoS), le trafic entrant ciblant la victime provient de plusieurs sources différentes - potentiellement des centaines de milliers ou plus.

Doxing – Pratique consistant à rechercher, ou pirater, des informations personnelles d'une personne sur l'Internet, puis les publier.

Malware – logiciel ou code malveillant. Les logiciels malveillants incluent les virus, les vers, les chevaux de Troie et les logiciels espions.

Les virus sont des programmes informatiques malveillants qui peuvent se propager à d'autres fichiers.

Un ver informatique est un programme malveillant autonome qui se réplique lui-même afin de se propager à d'autres ordinateurs. Souvent, il utilise un réseau informatique pour se propager, en s'appuyant sur des failles de sécurité sur l'ordinateur cible pour y accéder. Contrairement à un virus informatique, il n'a pas besoin de s'attacher à un programme existant.

Un cheval de Troie est tout programme informatique malveillant qui est utilisé pour pirater un ordinateur en trompant les utilisateurs de sa véritable intention.

Espiogiciel est un logiciel qui permet à un utilisateur d'obtenir des informations confidentielles sur les activités informatiques d'un autre en transmettant des données secrètement à partir de leur disque dur.

Phishing (hameçonnage) - l'utilisation d'e-mails qui semblent provenir d'une source de confiance, pour tromper les destinataires en cliquant sur les liens malveillants ou des pièces jointes contenant des logiciels malveillants, ou de partager des informations sensibles, avec un tiers inconnu.

Ransomware (Rançongiciel): logiciel malveillant qui empêche l'utilisateur d'accéder à ses fichiers, à son ordinateur ou à son périphérique jusqu'à ce qu'une rançon soit payée.

SMS spoofing – une technique qui permet de masque l'origine d'un SMS en replaçant le numéro de mobile par un texte alphanumérique. Il peut être utilisé légitimement par un expéditeur pour remplacer son numéro de téléphone portable par son nom propre, ou le nom de l'entreprise, par exemple. Il peut aussi être utilisé illégitimement, par exemple, pour se faire passer pour une autre personne.

Ingénierie Sociale – Méthode utilisée par des attaquants pour tromper et manipuler les victimes en exécutant une action ou en divulguant des informations confidentielles. Généralement, ces actions incluent l'ouverture d'une page Web malveillante ou l'exécution d'une pièce jointe indésirable.

Vulnérabilité - bogues dans les logiciels qui peuvent être exploités par des pirates informatiques.

Tests de vulnérabilité - Technique de test de logiciel permettant d'identifier, de quantifier et de hiérarchiser les vulnérabilités d'un système. Il est conseillé de procéder régulièrement à des tests de vulnérabilité car la grande majorité des vulnérabilités exploitées sont compromises plus d'un an après la publication de la vulnérabilité.