souveraine[MC]
ASSURANCE

25 Termes de cybersécurité

Que votre équipe de sécurité TI ne devrait pas être seule à connaître

Si vous ne croyez pas que votre entreprise ait été victime d'une cyberattaque, c'est que votre équipe de sécurité TI fait un excellent travail. En fait, il ne s'agit pas de déterminer « si » une entreprise sera victime d'une attaque, mais bien « quand ». La cybersécurité ne repose pas uniquement sur les épaules de votre équipe de TI. C'est la responsabilité de tous et toutes. Voici un glossaire de termes pour aider tout le personnel à peaufiner ses connaissances terminologiques en cybersécurité. Plus vous en saurez, plus vous pourrez en faire pour atténuer les cyberrisques.

1. Black hat
chapeau noir

Pirate informatique qui s'introduit dans un réseau pour voler de l'information qui sera utilisée de façon préjudiciable contre le propriétaire ou les utilisateurs sans leur consentement.

2. Bot/Botnet
contraction de « robot » et de « réseau de robots »

type d'application logicielle ou de script exécutant des tâches sur commande et permettant ainsi à l'auteur d'une attaque de prendre entièrement le contrôle à distance d'un ordinateur atteint. Un réseau de tels mécanismes d'infection et de contrôle d'ordinateurs est connu sous le nom de « botnet » (réseau de robots).

3. Business email compromise (BEC)
détournement de clic

Utilisation par un pirate informatique d'un compte de courriel d'entreprise pour se faire passer pour le vrai propriétaire afin de tromper des fournisseurs, des clients, des associés, etc. et de les inciter à envoyer de l'argent ou des données confidentielles dans le compte de l'auteur de l'attaque.

4. Clickjacking
détournement de clic

Attaque de piratage incitant les victimes à cliquer sur un lien sur un lien ou un bouton indésirable, habituellement présenté sous la forme d'un élément inoffensif.

5. Cloud *informatique en nuage*	technologie permettant aux utilisateurs d'accéder à des fichiers ou à des services (stockage de données) par Internet depuis n'importe quel endroit du monde.
6. Cryptage des données	Processus de chiffrement de données pour en prévenir le vol en faisant en sorte que les données ne soient accessibles qu'à l'aide d'une clé (c.-à-d. clé de déchiffrement) ou d'un mot de passe.
7. Déni de service distribué	Forme de cyberattaque ayant pour but de rendre indisponible un service, comme un site Web, en l'« inondant » de circulation ou de données malveillantes de sources multiples (souvent des botnets).
8. Déchiffrement	Conversion de données cryptées en vue d'en retrouver la forme originale.
9. Deepfake *hypertrucage*	image, fichier audio ou fichier vidéo modifié ou manipulé de façon à sembler véridique. Les cybercriminels peuvent utiliser ce contenu sur les réseaux d'information (p. ex., les réseaux sociaux) en vue de déployer des attaques de cybersécurité.
10. Domaine	Groupe d'ordinateurs, d'imprimantes et d'appareils interreliés et gérés comme constituant un tout.
11. Exploit	Application ou script malveillant permettant d'exploiter la vulnérabilité d'un ordinateur.
12. Pare-feu	Technologie défensive conçue pour prévenir les accès non autorisés. Un pare-feu peut être de nature matérielle ou logicielle.
13. Sécurité de l'internet des objets (IdO)	Technologie visant la protection des réseaux et des appareils branchés dans le domaine de l'Internet des objets (IdO). Les systèmes d'Internet des objets sont susceptibles à des attaques comme les dénis de services et l'ingénierie sociale.
14. Plan de réponse aux incidents	Procédures visant à aider le personnel des TI à détecter les incidents menaçant la sécurité des réseaux, à intervenir en conséquence et à rétablir les systèmes.
15. Menace interne	Menace à l'intégrité des données d'une entreprise émanant d'une personne de l'organisation.

16. Logiciel malveillant	terme générique englobant toutes les formes de programmes malveillants conçus pour semer le chaos dans un ordinateur, notamment les virus, les chevaux de Troie, les vers informatiques et les rançongiciels.
17. Correctif logiciel	Petite partie de logiciel lancée par une entreprise pour régler une faille de sécurité.
18. Test de pénétration	Méthode d'évaluation de la sécurité consistant à utiliser des techniques et des outils employés par les pirates dans le but de déceler les vulnérabilités et de mesurer les failles de sécurité que pourrait exploiter l'auteur d'une attaque.
19. Hameçonnage	technique par laquelle les cybercriminels envoient de faux courriels, messages textes ou sites Web qui ressemblent à s'y méprendre à une correspondance légitime afin de tromper les employés et d'accéder aux systèmes informatiques ou aux renseignements de l'entreprise.
20. Rançon	Forme de logiciel malveillant qui vous empêche délibérément d'accéder aux fichiers qui se trouvent sur votre ordinateur, prenant ainsi vos données en otage.
21. Ingénierie sociale	Forme de manipulation psychologique ciblant l'utilisateur plutôt que l'ordinateur en soi. Les cybercriminels tentent ainsi de tromper les gens pour accéder à des renseignements délicats et confidentiels.
22. Logiciel espion	Type de logiciel malveillant qui fonctionne envespionnant l'activité de l'utilisateur à son insu.
23. Authentification multi-facteurs	Processus de sécurité demandant à l'utilisateur de fournir deux facteurs d'authentification distincts tpour s'identifier (on parle parfois de « vérification en deux étapes »).
24. Fraude au fournisseur	Attaque visant la prise de contrôle du compte de courriel d'un fournisseur.
25. White hat *chapeau blanc*	Pirate informatique éthique ou expert en sécurité informatique embauché pour tester les vulnérabilités de l'infrastructure d'une organisation.