Glossaire des cyber expressions

Voici les cyber expressions courantes et leurs définitions.

Menace persistante avancée (MPA)
Cette expression désigne généralement un type avancé de cyber-attaque caractérisée par plusieurs méthodes intégrées d'une sophistication accrue suffisante pour imprégner toute défense périmétrique. Elle est également utilisée pour désigner les groupes qui effectuent ce style d'attaques sophistiquées tel que, mais ne se limitent plus à, un gouvernement étranger. La caractéristique des attaquants MPA est la capacité et l'intention de cibler de manière persistante et efficace une entité spécifique. L'expression est souvent utilisée pour désigner l'espionnage sur Internet qui utilise une variété de techniques de collecte de renseignements afin d'accéder aux renseignements sensibles, mais elle s'applique également à d'autres menaces comme celles de l'espionnage ou l'attaque traditionnelle. Les autres vecteurs d'attaque reconnus comprennent les supports contaminés, la compromission de la chaîne d'approvisionnement et l'ingénierie sociale. En général, une personne, comme un pirate informatique individuel, n'est pas désignée comme un MPA car une personne seule dispose rarement des ressources pour constituer à la fois une menace avancée et persistante, même si elle est résolue à obtenir l'accès à une cible spécifique ou à l'attaquer.

Logiciel publicitaire
Une forme de logiciel malveillant qui affiche des publicités indésirables à l'utilisateur de l'ordinateur, souvent en lançant de nombreuses annonces-éclair dans le navigateur de l'utilisateur. Un logiciel malveillant est souvent une forme de logiciel espion, surveillant l'activité de l'ordinateur et collectant des renseignements sans le consentement de l'utilisateur. Le terme logiciel publicitaire est également utilisé pour décrire un logiciel légitime gratuit ou à faible coût financé par la publicité.

Estimation des pertes annuelles (ALE)
La perte financière annuelle due à une menace prévue pour une organisation. Estimation de perte unique (SLE) X Taux annualisé d'occurrence (ARO) = Estimation des pertes annuelles (ALE).

Taux annualisé d'occurrence (ARO)
Une valeur qui représente la fréquence estimée à laquelle une menace devrait se produire. Celle-ci peut aller de 0 jusqu'à un très grand nombre. Par exemple, une éruption volcanique cataclysmique détruisant l'ensemble des installations pourrait se produire une fois tous les 100 000 ans et aurait un ARO de 0,00001. Alors que la fréquence estimée à laquelle 100 employés accèdent à des pages Web contenant des charges malveillantes pourrait être estimée à 5 fois par an et par salarié, ce qui donnerait un ARO de 500.

Logiciel antivirus
Un programme qui surveille un ordinateur ou un réseau dans le but d'empêcher, identifier et supprimer des logiciels malveillants.

Actif
Une ressource, processus, produit ou autre élément tangible d'information qu'une entreprise a décidé de protéger. La perte de l'actif pourrait avoir une incidence sur l'ensemble de la triade CIA (confidentialité, intégrité et disponibilité de l'information) ou elle pourrait avoir une valeur monétaire distincte.

Traitement automatique des données (TAD)
L'assemblage de matériel informatique, micrologiciels et logiciels utilisés pour classer, trier, compter, calculer, résumer, stocker, récupérer, contrôler, traiter ou protéger les données avec le minimum d'intervention humaine.

Opération de sauvegarde
Un mode de fonctionnement qui permet d'accomplir des tâches essentielles telles qu'identifiées par une analyse des risques. Ces tâches seraient utilisées à la suite d'une perturbation du SIG et se poursuivraient jusqu'à ce que le SIG soit restauré de manière acceptable.

Données volumineuses
Un terme général utilisé pour décrire la quantité volumineuse de données non structurées et semi-structurées qu'une entreprise crée — des données qui prendraient trop de temps et coûteraient trop d'argent à charger dans une base de données relationnelle pour analyse. Bien que le terme « données volumineuses » ne fasse pas référence à une quantité spécifique, il est souvent utilisé lorsqu'on parle de pétaoctets et d'exaoctets de données.

L'objectif principal pour examiner les données volumineuses est de découvrir des modèles d'activités reproductibles. Il est en général admis que les données non structurées, situées pour la plupart dans des fichiers texte, représentent au moins 80 % des données de l'entreprise. S'il n'est pas géré, le volume pur des données non structurées générées chaque année au sein d'une entreprise peut être coûteux en termes de stockage. Des données non gérées peuvent également être une source de responsabilité si les renseignements ne peuvent pas être localisés dans le cas d'une vérification de la conformité ou d'un procès.

L'analyse des données volumineuses est souvent associée à l'informatique en nuage, car l'analyse de grands ensembles de données en temps réel nécessite un cadre afin de répartir le travail parmi des dizaines, des centaines ou même des milliers d'ordinateurs.

Chapeau noir
Ce terme trouve son origine dans les films de western, où le méchant ou le mauvais garçon porte un chapeau noir par opposition au chapeau blanc porté par le héros. L'expression est souvent utilisée au sens figuré, en particulier en argot informatique où elle fait référence à un pirate informatique qui viole des réseaux ou des ordinateurs, ou crée des virus informatiques à des fins malveillantes.

Bluebugging
Une forme d'attaque Bluetooth. Un programme Bluebug permet à l'utilisateur de prendre le contrôle du téléphone de la victime. En plus de pouvoir émettre des appels, ils peuvent également envoyer des messages et essentiellement faire tout ce que le téléphone peut faire. Cela signifie également que l'utilisateur Bluebug peut tout simplement écouter n'importe quelle conversation de sa victime.

Bluejacking
Envoi de messages non sollicités via le Bluetooth à des périphériques Bluetooth compatibles, tels que des téléphones mobiles, assistants numériques personnels ou ordinateurs portables.

Bluesnarfing
L'accès non autorisé aux informations provenant d'un appareil sans fil via une connexion Bluetooth, souvent entre les téléphones, ordinateurs de bureau, ordinateurs portables et les assistants numériques personnels. Ceci permet d'accéder au calendrier, à la liste de contacts, courriels et messages texte, et sur certains téléphones les utilisateurs peuvent voler des photos et des vidéos privées.

Botnet
Un terme du jargon informatique pour désigner un réseau d'ordinateurs et de robots logiciels, ou bots, qui fonctionnent de manière autonome et automatique. Ils fonctionnent sur des groupes d'ordinateurs zombies contrôlés à distance. Un ordinateur peut être ajouté sans le savoir à un botnet à la suite d'une intrusion de logiciels malveillants. Le créateur ou le propriétaire du botnet peut ensuite utiliser le réseau pour des activités malveillantes, généralement pour des attaques par déni de service.

Loi anti-pourriels (CAN-SPAM Act)
Une loi qui fixe les règles pour les courriels commerciaux, établit des conditions pour les messages publicitaires, donne aux destinataires le droit de vous faire cesser de leur envoyer des courriels et qui énonce des sanctions sévères en cas d'infractions. Malgré son nom, la loi anti-pourriels (CAN-SPAM Act) ne s'applique pas uniquement aux courriels d'envoi en masse. Elle couvre tous les messages publicitaires que la Loi définit comme message de courrier électronique ayant pour objectif principal la publicité commerciale ou la promotion d'un produit ou service commercial, y compris les courriels faisant la promotion de contenu sur les sites Web commerciaux. La loi ne fait aucune exception pour les courriels entreprise à entreprise. Cela signifie que tous les courriels – par exemple, un message aux anciens clients annonçant une nouvelle gamme de produits – doivent respecter la Loi. Chaque courriel distinct enfreignant la loi anti-pourriels (CAN-SPAM Act) est passible de sanctions pouvant atteindre jusqu'à 16 000 $.

CERT
Acronyme dérivé de « Computer Emergency Response Team », l'équipe d'intervention en cas d'urgence informatique de l'Université Carnegie Mellon (CMU). Le programme CERT développe et promeut l'utilisation des technologies et des pratiques de gestion des systèmes appropriées afin de résister aux attaques sur les systèmes en réseau, de limiter les dommages et d'assurer la continuité des services essentiels. De nombreuses équipes CERT sont maintenant déployées partout dans le monde afin d'effectuer des fonctions similaires, bien que toutes ne se soient pas rattachées à la CMU.

Environnement de données des titulaires de carte
Les personnes, les processus et les technologies qui stockent, traitent ou transmettent les données des titulaires de carte ainsi que les données sensibles d'authentification, y compris les composants du système connecté.

Effacer ou effacement (supports de stockage du SIG)
La suppression des données d'un système d'information, de ses périphériques de stockage et d'autres appareils périphériques ayant une capacité de stockage, d'une façon telle que les données ne peuvent pas être reconstruites en utilisant les capacités communes du système (c'est-à-dire par le clavier) ; toutefois, les données peuvent être reconstruites à l'aide de méthodes de laboratoire.

Fraude au clic
Un type de cybercriminalité qui se produit dans la publicité en ligne à paiement au clic lorsqu'une personne, un script automatisé ou programme informatique imite un utilisateur légitime d'un navigateur Web en cliquant sur une annonce, dans le but de générer une redevance par clic sans avoir un intérêt réel dans la cible du lien de l'annonce. La fraude au clic fait l'objet de certaines controverses et de contentieux croissants du fait que les réseaux publicitaires en sont les principaux bénéficiaires.

Informatique en nuage
L'informatique en nuage est un terme général pour tout ce qui implique la fourniture de ressources informatiques hébergées sur l'Internet (ou autre grand réseau). Ces services sont souvent répartis en trois grandes catégories : Infrastructure en tant que service (IaaS), plateforme en tant que service (PaaS) et logiciel en tant que service (SaaS). La dénomination « informatique en nuage » s'inspire du symbole du nuage qui est souvent utilisé pour représenter l'Internet dans les organigrammes et diagrammes. Un service infonuagique possède trois caractéristiques distinctes le différenciant des hébergements traditionnels. Il est vendu à la demande, en général à la minute ou à l'heure ; il est élastique, un utilisateur peut avoir autant ou aussi peu de service qu'il le souhaite à tout moment ; et peut être entièrement géré par le fournisseur (le consommateur n'a besoin que d'un ordinateur personnel et d'un accès Internet). Les innovations importantes dans la virtualisation et l'informatique distribuée, l'amélioration de l'accès à l'Internet haut débit et la faiblesse de l'économie ont accéléré l'intérêt pour l'informatique en nuage.

Produit informatique standard ou produit informatique COTS
Désigne les produits qui sont disponibles sur le marché et qui peuvent être utilisés tels que généralement commercialisés par le fabricant.

Virus informatique
Un programme informatique qui peut se dupliquer et infecter un ordinateur sans l'autorisation ou à l'insu de l'utilisateur. Le terme « virus » est également couramment utilisé, mais à tort, pour désigner différents types de logiciels malveillants et logiciels publicitaires.

Ver informatique
Un programme informatique auto-réplicatif. Il utilise un réseau pour envoyer des copies de lui-même à d'autres terminaux d'ordinateur sur le réseau et il peut le faire sans aucune intervention de l'utilisateur. Contrairement à un virus, il n'a pas besoin de se fixer à un programme existant. Les vers endommagent presque toujours le réseau, ne serait-ce qu'en consommant de la bande passante, alors que les virus corrompent ou modifient presque toujours les fichiers sur l'ordinateur ciblé. De nombreux vers créés ont été conçus uniquement pour se propager et n'essaient pas de modifier les systèmes qu'ils traversent. Cependant, comme les vers Morris et Mydoom l'ont démontré, le trafic sur le réseau et d'autres effets inattendus peuvent souvent entraîner des perturbations majeures.

Gestion de configuration
La gestion des modifications apportées au matériel SIG, logiciel, micrologiciel, documentation, essais, montages de tests, documents d'essai, interfaces de communication, procédures d'exploitation et structures de l'installation tout au long du cycle de développement et d'exploitation du SIG..

Protection contrôle d'accès (C2)
Ensemble minimal de fonctionnalités de sécurité qui impose un contrôle d'accès aux utilisateurs individuels et les rend responsables de leurs actions grâce à des procédures de connexion, la vérification des événements relatifs à la sécurité et l'isolation des ressources.

Témoin
Un petit fichier de données qu'un site Web installe sur le disque dur de votre ordinateur afin de recueillir des renseignements sur vos activités sur le site ou permettre d'autres fonctionnalités sur le site. Les sites Web utilisent des témoins pour identifier les visiteurs qui reviennent et connaitre leurs préférences sur le site. Par exemple, de nombreux sites de vente en ligne utilisent des témoins pour surveiller les articles qu'un client achète afin de suggérer des articles similaires. Les témoins sont quelque peu controversés, car ils soulèvent des questions concernant le respect de la vie privée et peuvent être utilisés par des pirates informatiques comme des logiciels espions.

Logiciel criminel
Programme informatique conçu spécifiquement pour mener des activités illégales en ligne.

Analyse cryptographique (cryptologie/cryptographie)
Les sciences mathématiques qui traitent de l'analyse d'un système de chiffrement (cryptage et décryptage) afin d'acquérir les connaissances nécessaires pour casser ou contourner la protection que la conception du système fournit sans connaître la clé.

Cyber
Un préfixe utilisé pour décrire une personne, une chose ou une idée ayant trait à des ordinateurs, des technologies de l'information ou à des systèmes d'information de gestion.

Cyber-assurance
Des produits d'assurance qui offrent une protection contre les risques liés aux systèmes informatiques, technologies de l'information, systèmes d'information de gestion, à la sécurité des réseaux et à l'utilisation et au stockage des données sensibles ou confidentielles. Ces risques comprennent (mais ne sont pas limités à) les violations des données sensibles, le piratage informatique, la fouille de poubelles, les virus informatiques et le sabotage ou le vol d'informations par les employés et l'usurpation d'identité.

Responsabilités liées au cyberespace
Les risques de première et de tierce partie pour les pays, les entreprises et les personnes associés aux ordinateurs, aux technologies de l'information, aux systèmes d'information de gestion et aux données sensibles. Ces risques comprennent (mais ne sont pas limités à) les violations des données sensibles, le piratage informatique, la fouille de poubelles, les virus informatiques et le sabotage ou le vol d'informations par les employés et l'usurpation d'identité.

Gestion des cyber-risques
Le processus de gestion des risques liés aux ordinateurs, aux technologies de l'information, aux systèmes d'information de gestion et aux données sensibles.

Cybersécurité
L'ensemble des technologies, des processus et des pratiques visant à protéger les ordinateurs, les technologies de l'information, les systèmes d'information de gestion et les données sensibles contre une attaque, des dommages ou un accès non autorisé.

CyberEdge®
La solution de gestion complète des risques de la cyber-assurance offerte par AIG. Dans un paysage en constante évolution, CyberEdge offre une protection innovante afin d'aider les entreprises à se protéger contre les violations des données sensibles, le piratage informatique, la fouille de poubelles, les virus informatiques et le sabotage ou les erreurs des employés, le vol d'informations et l'usurpation d'identité. CyberEdge aide les entreprises à garder une longueur d'avance et fournit des conseils adaptés fondés sur des années d'expérience. CyberEdge offre une protection supplémentaire aux plus puissantes premières lignes de défense des entreprises contre les cyber-menaces – leurs propres systèmes informatiques.

Cybercriminalité
Les délits qui sont commis contre des personnes ou des groupes de personnes avec un motif criminel afin de nuire intentionnellement à la réputation de la victime ou de causer un préjudice physique ou mental à la victime directement ou indirectement, à l'aide des réseaux de télécommunication modernes tels qu'Internet (bavardoirs, courriels, babillards et groupes) et les téléphones mobiles (SMS/MMS).

Droit du cyberespace
Le domaine en rapide évolution du droit civil et pénal s'appliquant à l'utilisation de l'ordinateur et d'Internet et à l'échange de communications et d'informations sur celui-ci, y compris les enjeux connexes concernant ces communications et informations tels que la protection des droits de propriété intellectuelle, la liberté d'expression et l'accès du public à l'information.

Cyber-harcèlement
L'utilisation d'internet pour surveiller ou harceler une personne ou un groupe de personnes. Le cyber-harcèlement consiste souvent en l'envoi répété de messages comportant des menaces de préjudice ou très intimidants et la participation à d'autres activités en ligne donnant à une personne une raison de craindre pour sa sécurité.

Violation de données
Un incident impliquant un accès non autorisé, un vol ou la divulgation de renseignements non publics.

Norme de chiffrage des données (DES)
Une méthode couramment utilisée de chiffrement des données à l'aide d'une clé privée (secrète). DES est un chiffrement par blocs de cryptage défini et approuvé par le gouvernement américain en 1977 en tant que norme officielle (FIPS PUB 59).

Attaque par déni de service (DoS)
Ou attaque par déni de service distribué (DDoS) est une tentative de rendre une ressource informatique indisponible à ses utilisateurs prévus. Bien que les moyens, les motivations et les cibles d'une attaque par déni de service puissent varier, elle consiste en général en des efforts concertés et malveillants d'une ou plusieurs personnes pour empêcher les utilisateurs légitimes d'utiliser un service en réseau en bloquant le service ou en inondant le service de demandes et/ou d'informations illégitimes.

Critères d'évaluation des systèmes informatiques protégés du Ministère de la défense (DOD)
Créés par le Centre national de sécurité informatique (NCSC), ces critères sont destinés à être utilisés dans la conception et l'évaluation des systèmes qui traiteront et/ou stockeront les données sensibles. Ce document contient un ensemble uniforme d'exigences fondamentales ainsi que les classes d'exploitation utilisées pour évaluer les degrés de confiance en l'efficacité des contrôles de sécurité du matériel et des logiciel intégrés dans la conception et l'évaluation des SIG.

Contrôle d'accès discrétionnaire (DAC)
Un moyen de restreindre l'accès aux objets en fonction de l'identité des sujets et/ou des groupes auxquels ils appartiennent ou de la possession d'une autorisation accordant l'accès à ces objets.

Mystification de courriel
Un terme utilisé pour décrire une activité de courrier électronique frauduleuse dans laquelle l'adresse de l'expéditeur et des autres parties de l'en-tête d'un courriel sont modifiées afin de faire croire que le courriel provient d'une source différente. La mystification de courriel est une technique couramment utilisée pour le courrier indésirable et l'hameçonnage afin de masquer l'origine du message électronique.

Cryptage ou chiffrement
Processus de conversion des informations en une forme inintelligible sauf aux détenteurs d'une clé de chiffrement spécifique. L'utilisation du chiffrement protège les informations entre le processus de chiffrement et le processus de déchiffrement (l'inverse du chiffrement) contre toute divulgation non autorisée.

Facteur d'exposition
Le pourcentage de perte qu'une menace réalisée aurait sur un actif particulier.

FIPS
Acronyme de Federal Information Processing Standards. Ce sont les normes publiquement reconnues par le gouvernement fédéral américain ; elles sont également utilisées par les organismes non gouvernementaux et les entrepreneurs.

Opérations sous fausse bannière
Opérations secrètes menées par des gouvernements, sociétés ou autres organismes conçues de manière à sembler avoir été commises par d'autres entités.

Pare-feu
Un ensemble de composants ou un système placé entre deux réseaux et possédant les propriétés suivantes : 1) tout le trafic de l'intérieur vers l'extérieur et réciproquement, doit le franchir ; 2) seul le trafic autorisé, tel que défini par la politique de sécurité locale, est autorisé à le franchir ; et 3) le système lui-même est à l'abri d'une intrusion.

Micrologiciel
Les programmes informatiques et les données qui sont stockés dans le matériel et ne peuvent pas être écrits ou modifiés dynamiquement lors de l'exécution des programmes ou des opérations normales de l'appareil.

Pirate informatique
Surnom courant d'une personne (ou organisation) non autorisée qui s'introduit ou tente de pénétrer dans un système d'information de gestion en contournant les mesures de sécurité des logiciels.

Hachage
Processus consistant à rendre les données de titulaire de carte illisibles en les convertissant en un message condensé de longueur fixe via une cryptographie forte. Le hachage est une fonction mathématique dans laquelle un algorithme non secret acquiert en entrée un message de longueur arbitraire et produit une sortie de longueur fixe. Une fonction de hachage doit posséder les propriétés suivantes : dans le cadre de la norme PCI DSS, le hachage doit être appliqué à la totalité du PAN entier pour que le code de hachage soit considéré comme illisible. Il est recommandé que les données de titulaire de carte hachées comprennent un sel en entrée à la fonction de hachage.

Usurpation d'identité
L'accès non autorisé à l'identité d'une personne afin de détourner l'argent, le crédit ou autres ressources de cette personne. L'usurpation d'identité se produit le plus souvent lorsqu'une personne non autorisée a accès aux renseignements personnels identifiables d'une autre personne afin de commettre une fraude ou d'autres crimes.

Loi sur la communication et la coopération internationales sur la cybercriminalité
Une législation bipartisane présentée par les sénateurs Orrin Hatch (R-UT) et Kirsten Gillibrand (D-NY) pour améliorer la coopération des États-Unis avec d'autres pays afin d'affronter cette menace.

Système de détection d'intrusion (SDI)
Logiciel ou matériel utilisé pour identifier les tentatives d'intrusion dans un réseau ou un système et donner l'alerte. Constitué de capteurs qui génèrent des événements de sécurité ; d'une console pour surveiller les événements et les alertes et contrôler les capteurs ; et d'un moteur central qui enregistre les événements consignés par les capteurs dans une base de données. Utilise un système de règles pour déclencher des alertes en réponse aux événements de sécurité détectés.

Centre de distribution de clés
Un système qui est autorisé à transmettre les clés de sessions temporaires aux responsables (utilisateurs autorisés) afin de réduire les risques inhérents à l'échange de clés. Chaque clé de session est transmise sous forme cryptée, à l'aide d'une clé principale que la distribution de clés partage avec le responsable cible.

Enregistreur de frappe
Une méthode de capture et d'enregistrement des frappes de l'utilisateur. L'enregistrement de frappe peut être utile pour définir les sources d'erreurs dans les systèmes informatiques, afin d'étudier la façon dont les utilisateurs interagissent et accèdent aux systèmes et est parfois utilisé pour mesurer la productivité des employés sur certaines tâches administratives. Ces systèmes sont également très utiles pour l'application de la loi et l'espionnage — par exemple, en offrant le moyen d'obtenir les mots de passe ou les clés de chiffrement et de contourner ainsi les autres mesures de sécurité.

Sécurité des systèmes d'information
Les mesures ou les contrôles qui protègent ou préservent un système d'information de gestion contre une divulgation non autorisée accidentelle ou intentionnelle, une modification, une destruction du SIG et des données, ou une attaque par déni de service. La sécurité des systèmes d'information (MIS security) fournit un niveau de risque acceptable pour le SIG et les données qu'il contient.

Code malveillant
Logiciel ou micrologiciel qui est intentionnellement inclus dans un système d'information de gestion à des fins non autorisées.

Logiciel malveillant
Un programme qui est inséré dans un système, en général secrètement, avec l'intention de compromettre la confidentialité, l'intégrité ou la disponibilité des données des utilisateurs, des applications ou du système d'exploitation ou autrement d'ennuyer ou perturber l'utilisateur.

Système d'information de gestion (SIG)
Un assemblage de matériel informatique, de logiciels et/ou de micrologiciels configurés pour collecter, créer, communiquer, calculer, diffuser, traiter, stocker et/ou contrôler des données ou informations.

Marchand
Dans le cadre de la norme PCI DSS, un marchand est défini comme une entité qui accepte les cartes de paiement portant le logo de l'un des cinq membres du PCI SSC (American Express, Discover, JCB, MasterCard ou Visa) comme moyen de paiement de marchandises et/ou de services. Notez qu'un commerçant qui accepte ces cartes de paiement comme moyen de paiement des marchandises et/ou des services peut également être un prestataire de services, si les services vendus entraînent le stockage, le traitement ou la transmission des données de titulaires de carte au nom d'autres marchands ou prestataires de services. Par exemple, un FAI est un marchand qui accepte les cartes de paiement pour la facturation mensuelle, mais est également un prestataire de services s'il héberge des marchands en tant que clients.

Institut national des normes et de la technologie (National Institute of Standards and Technology)
Une unité du Département du commerce des États-Unis et anciennement connu sous l'appellation Bureau national des normes, le NIST promeut et maintient les étalons de mesure, encourage et aide également l'industrie et la science à élaborer et à utiliser ces normes.

Politique nationale de sécurité des systèmes de télécommunications et d'information
Directive pour les organismes fédéraux, à compter du 15 juillet 1992, en vue de fournir une Protection automatisée de contrôle d'accès (niveau C2) au SIG, lorsque les utilisateurs n'ont pas tous la même autorisation pour utiliser les renseignements de nature délicate.

Assurance de sécurité et de confidentialité du réseau
Protection des réseaux et de leurs services contre la modification non autorisée, la destruction, la divulgation et la garantie que le réseau exécute ses fonctions essentielles correctement et qu'il n'y a aucuns effets secondaires nocifs. L'assurance protection de la vie privée offre une protection contre les dépenses et les responsabilités légales associées aux atteintes à la sécurité de la vie privée.

Fraude 419 ou arnaque nigériane
Un abus de confiance dans lequel la cible est persuadée d'avancer des sommes d'argent relativement petites dans l'espoir de réaliser un plus grand gain.

Procédure d'écrasement
Un processus qui supprime ou détruit les données enregistrées sur un support de stockage informatique en écrivant des modèles de données sur, ou au-dessus des données stockées sur le support.

Carte de paiement
Dans le cadre de la norme PCI DSS, toute carte ou dispositif de paiement portant le logo des membres fondateurs de la norme PCI SSC, soit American Express, Discover Financial Services, JCB International, MasterCard Worldwide, ou Visa.

Norme de sécurité de l'industrie des cartes de paiement (PCI DSS)
La norme mondiale de sécurité des données que toute entreprise, quelle que soit sa taille, doit respecter afin d'accepter ou de traiter des transactions par carte de paiement. La norme comprend douze exigences pour toute entreprise qui stocke, traite ou transmet les données des titulaires de carte de paiement.

Conseil des normes de sécurité de l'industrie des cartes de paiement

Le Conseil des normes de sécurité de l'industrie des cartes de paiement, ou PCI SSC est un forum mondial ouvert lancé en 2006, qui élabore, maintient et gère les normes de sécurité PCI, qui comprennent la norme de sécurité des données (DSS), la norme de sécurité des données d'application de paiement (PA-DSS) et les exigences relatives à la sécurité des transactions par code PIN (PTS). Le Conseil s'efforce de sensibiliser les intervenants aux normes de sécurité PCI, gère les programmes visant à former et qualifier les professionnels de la sécurité en évaluation et mise en conformité aux normes de sécurité PCI et favorise la sensibilisation au besoin de sécurité des données de paiement pour le public.

Les cinq marques de paiement mondiales fondatrices du Conseil : American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa – ont intégré les normes PCI DSS en exigences techniques pour leurs programmes de conformité de sécurité des données. Chaque membre fondateur reconnaît également les professionnels et les entreprises – évaluateurs de sécurité qualifiés et prestataires de services d'analyse agréés – certifiés par le Conseil des normes de sécurité PCI comme étant qualifiés pour valider la conformité à la norme PCI DSS, contribuant à faire du Conseil une ressource centralisée pour l'accès aux normes et aux services approuvés par les cinq marques de paiement.

Données personnelles identifiables (DPI)
Renseignements pouvant être utilisés pour identifier, contacter ou localiser une personne en particulier, soit seuls ou lorsque combinés avec d'autres renseignements personnels ou d'identification. Les DPI peuvent inclure le nom, l'adresse, les numéros de téléphone, le numéro d'assurance sociale, le numéro de compte bancaire, le numéro de compte de la carte de crédit, les noms des membres de la famille ou les noms des amis d'une personne. Les pirates informatiques qui cherchent à voler une identité ou de l'argent ont souvent pour objectif de trouver ces renseignements.

Hameçonnage
Désigne une tentative d'acquérir de manière frauduleuse et criminelle des renseignements sensibles, tels que les noms d'utilisateur, les mots de passe et les renseignements de la carte de crédit, en se faisant passer pour une entité digne de confiance lors d'une communication électronique. PayPal, eBay et les banques en ligne sont des cibles courantes. L'hameçonnage est généralement effectué par courriel ou messagerie instantanée et dirige souvent les utilisateurs vers un site Web pour y entrer les renseignements, bien que le contact téléphonique soit aussi utilisé.

Piggybacking (Superposition)
Un terme utilisé pour désigner l'accès à une connexion internet sans fil en mettant son propre ordinateur dans la portée de connexion sans fil d'un autre ordinateur et en utilisant ce service sans l'autorisation explicite ou à l'insu de l'abonné. Il s'agit d'une pratique juridiquement et éthiquement controversée, avec des lois qui varient selon les pays dans le monde. Alors que cette pratique peut être complètement illégale dans certaines juridictions, elle est autorisée dans d'autres pays. Le Piggybacking est utilisé comme un moyen de cacher des activités illégales, telles que le téléchargement de pornographie enfantine ou un vol d'identité par exemple. Il s'agit d'une des raisons principales de la controverse.

Siphonage Pod
Le fait d'utiliser un périphérique de stockage des données portable comme un lecteur audio numérique iPod afin de télécharger illégalement de grandes quantités de données confidentielles, en le branchant directement dans l'ordinateur où les données sont conservées et qui peuvent se trouver à l'intérieur d'un pare-feu. Alors que ces dispositifs de stockage deviennent plus petits et que leur capacité de stockage augmente, ils représentent un risque de sécurité accru pour les entreprises et les agences gouvernementales. L'accès est obtenu lorsque l'ordinateur est laissé sans surveillance.

Renseignements médicaux protégés (PHI)
Les renseignements médicaux identifiables à titre individuel qui sont liés à la santé, ou à l'état physique ou mental passé, présent et futur d'une personne, à la prestation de soins de santé à une personne, ou au paiement passé, présent ou futur des soins de santé fournis à une personne. Les renseignements médicaux protégés (PHI) sont protégés en vertu des normes de l'HIPAA.

Droit public 100-235
Établit les normes minimales acceptables en matière de sécurité informatique et de confidentialité des renseignements personnels.

Évaluation qualitative du risque
Essaie de classer le niveau de gravité des menaces perçues et ce faisant, classe ou hiérarchise qualitativement la sensibilité relative d'un actif.

Analyse quantitative des risques
Essaie d'attribuer de façon indépendante des valeurs numériques objectives (monétaires) aux composantes de l'évaluation des risques et à l'évaluation des pertes potentielles.

Risque résiduel
Le risque potentiel restant après l'application de toutes les mesures de sécurité informatique. Il existe un risque résiduel associé à chaque menace.

Gestion des risques [évaluation des risques]
Le processus de gestion/identification des risques pour les activités organisationnelles (y compris la mission, les fonctions, l'image et la réputation), les actifs organisationnels, les personnes, les autres organismes et la nation, découlant de l'exploitation d'un système d'information. Remarque : l'analyse des risques fait partie de la gestion des risques et est synonyme d'évaluation des risques.

Programmes malveillants furtifs
Un programme conçu pour acquérir le contrôle fondamental (accès root dans Unix, accès administrateur dans Windows) d'un système informatique, sans l'autorisation des propriétaires et des gestionnaires légitimes du système. L'accès au matériel est rarement nécessaire car les programmes malveillants furtifs sont destinés à prendre le contrôle du système d'exploitation s'exécutant sur le matériel. En règle générale, les programmes malveillants furtifs agissent de manière à masquer leur présence sur le système par la subversion ou le contournement des mécanismes standards de sécurité du système d'exploitation. Ils sont aussi souvent des chevaux de Troie, trompant ainsi les utilisateurs en leur faisant croire qu'ils exploitent leurs systèmes en toute sécurité. Les techniques utilisées pour y parvenir peuvent comprendre la dissimulation des processus en cours d'exécution à partir des programmes de surveillance, ou le masquage des fichiers ou des données système à partir du système d'exploitation.

Guide SEC de cybersécurité a/k/a Guide de divulgation CF : rubrique N° 2, Cybersécurité
En octobre 2011, la Division of Corporation Finance du SEC a fourni des directives concernant les obligations de divulgation relatives aux risques de cybersécurité, incidents cybernétiques et à l'assurance. Pour l'essentiel, la directive indique que bien qu'aucune exigence de divulgation existante ne fasse explicitement référence aux risques de cybersécurité et aux incidents cybernétiques :

1. un certain nombre d'obligations de divulgation peuvent imposer aux déclarants l'obligation de divulguer ces risques et incidents ; et
2. Les renseignements importants concernant les risques de cybersécurité et les incidents cybernétiques doivent être divulgués si nécessaire afin de rendre les autres divulgations requises non équivoques, à la lumière des circonstances dans lesquelles elles sont faites.

Selon les faits et les circonstances particulières du déclarant et dans la mesure où elles sont importantes, les divulgations appropriées peuvent comprendre : la discussion sur les aspects des affaires ou des activités du déclarant qui entraînent des risques importants de cybersécurité ainsi que les coûts et conséquences éventuels ; dans la mesure où le déclarant sous-traite des fonctions comportant des risques importants de cybersécurité, la description de ces fonctions et de la manière dont le déclarant traite ces risques ; la description des incidents cybernétiques vécus par le déclarant qui sont individuellement, ou globalement, matériels, y compris la description des coûts et autres conséquences ; les risques liés aux incidents cybernétiques qui pourraient ne pas être détectés pendant une période prolongée ; et la description de la couverture d'assurance pertinente.

Injection de commandes SQL
Une attaque informatique par laquelle un code malveillant est intégré dans une application mal conçue et est transmis à la base de données dorsale. Les données malveillantes produisent ensuite des résultats ou des actions de requêtes de base de données qui n'auraient jamais dû être exécutées.

Protection
Un contrôle ou une contre-mesure d'atténuation conçue et utilisée pour réduire les risques associés à une menace spécifique ou à un groupe de menaces.

Exigences de sécurité
Les types et les niveaux de protection nécessaires pour le matériel, les données, les informations, les applications et les installations afin de satisfaire aux politiques en matière de sécurité.

Spécifications de sécurité
Une description détaillée des protections de sécurité nécessaires pour protéger un système.

Atteinte à la sécurité
Un événement pouvant entraîner la divulgation de renseignements sensibles à des personnes non autorisées, ou une modification ou destruction non autorisée des données du système, la perte de la capacité de traitement du système informatique, ou la perte ou le vol des ressources du système informatique.

Prestataire de services
Une entité commerciale qui n'est pas une marque de paiement, directement impliquée dans le traitement, le stockage ou la transmission des données de titulaires de carte. Cela comprend également les sociétés qui fournissent des services qui contrôlent, ou pourraient avoir une incidence sur la sécurité des données des titulaires de carte. Les exemples incluent les prestataires de services gérés qui fournissent des pare-feux gérés, des services SDI et autres ainsi que les fournisseurs d'hébergement et autres entités. Les entités telles que les sociétés de télécommunications qui fournissent uniquement des liaisons de communication sans accès à la couche d'application de la liaison de communication sont exclues.

Estimation de perte unique
Le montant qui est attribué à un événement unique. Elle représente la perte de l'entreprise provenant d'un cas isolé de menace. Valeur de l'actif ($) x Facteur d'exposition (EF) = Estimation de perte unique (SLE).

Ingénierie sociale
L'art de manipuler les personnes dans la réalisation d'actions ou la divulgation de renseignements confidentiels. Bien que semblable à un abus de confiance ou à une simple fraude, le terme s'applique en général à une supercherie visant à recueillir des renseignements ou un accès au système informatique et dans la plupart des cas, l'attaquant ne se trouve jamais en face de la victime.

Logiciel de craquage
La modification du logiciel afin de supprimer les modes de protection : prévention de la copie, version d'essai/démonstration, numéro de série, clé électronique, vérification de CD ou ennuis logiciels comme les écrans intempestifs et les logiciels publicitaires.

Pollupostage
L'abus des systèmes de messagerie électronique pour envoyer sans discernement des messages en masse non sollicités. Alors que la forme la plus largement répandue de pourriels est l'envoi de courriels non sollicités, le terme s'applique à des abus similaires dans d'autres médias : pourriel de messagerie instantanée, pourriel Usenet newsgroup, pourriel de moteur de recherche Web, pourriel dans les blogs, pourriel de wiki, pourriel de messagerie sur téléphone mobile, pourriel de forum Internet et transmissions de télécopies indésirables.

Harponnage
Des versions ciblées d'hameçonnage ont été appelées harponnage. Plusieurs attaques récentes d'hameçonnage ont visé spécifiquement des cadres supérieurs et autres cibles de grande notoriété au sein des entreprises et le terme « chasse à la baleine » a été inventé pour ces types d'attaques.

Logiciels espions
Logiciel installé secrètement dans un système d'information de gestion afin de recueillir des informations sur des individus ou des entreprises à leur insu ; un type de code malveillant.

Système autonome
Un utilisateur SIG unique non connecté aux autres systèmes.

Procédures de sécurité standard
Instructions de sécurité détaillées adaptées aux utilisateurs et aux opérateurs de SIG qui traitent des renseignements sensibles.

Stealware
Désigne un type de logiciel qui transfère réellement les sommes dues à un propriétaire de site Web à un tiers. Plus précisément, le « stealware » utilise un témoin de connexion HTTP pour détourner la commission qu'un site Web a gagnée en référençant ses utilisateurs vers un autre site.

Chiffrement symétrique
Une forme de cryptographie, dans laquelle le chiffrement et le déchiffrement sont effectués en utilisant la même clé.

Intégrité du système
L'attribut d'un système relatif à l'utilisation efficace et correcte des ressources informatiques.

Menace
La survenance de tout événement qui entraîne des répercussions indésirables sur l'entreprise. Les menaces peuvent être d'origine humaine ou naturelle.

Agent de menace
Une personne ou une chose, qui agit, ou a le pouvoir d'agir, de provoquer, transporter, transmettre ou soutenir une menace.

Cheval de Troie
Logiciel qui semble effectuer une certaine action mais qui en fait en effectue une autre comme la transmission d'un virus informatique. Contrairement à la croyance populaire, cette action, généralement encodée dans une charge cachée, peut ou peut ne pas être réellement malveillante, mais les chevaux de Troie sont connus aujourd'hui pour leur utilisation dans l'installation de programmes de porte dérobée. Autrement dit, un cheval de Troie n'est pas un virus informatique. Contrairement à ces logiciels malveillants, il ne se propage pas par auto-réplication, mais repose fortement sur l'exploitation d'un utilisateur final (voir ingénierie sociale).

Système informatique fiable (TCSEC)
Un système qui utilise des mesures appropriées de la confiance dans le matériel et les logiciels afin de permettre leur utilisation pour le traitement d'un éventail de renseignements sensibles ou classifiés simultanément.

Alimentation sans coupure (UPS)
Un système de composants électriques pour fournir un tampon entre le réseau électrique, ou une autre source d'alimentation et une charge qui nécessite une alimentation ininterrompue et précise.

Virus
Un programme qui s'attache à un fichier exécutable ou à une application vulnérable et livre une charge allant de gênante à extrêmement destructrice. Un virus de fichier s'exécute lorsqu'un fichier infecté est ouvert. Un virus de macro infecte le code exécutable intégré dans les programmes Microsoft Office qui permet aux utilisateurs de créer des macros.

Hameçonnage vocal
Désigne la pratique criminelle qui consiste à utiliser l'ingénierie sociale et la Voix sur IP (VoIP) pour accéder aux renseignements personnels et financiers privés du public à des fins de rémunération financière. Le terme est une combinaison de voix et d'hameçonnage. L'hameçonnage vocal exploite la confiance du public dans les services de téléphonie fixe, qui ont traditionnellement une terminaison dans des emplacements physiques connus de la compagnie de téléphone et associés à un payeur. La victime ignore souvent que la VoIP permet l'usurpation d'identité de l'appelant par des systèmes automatisés complexes et peu coûteux et de lever l'anonymat du payeur. L'hameçonnage vocal est généralement utilisé pour voler des numéros de carte de crédit ou autres informations utilisées dans les systèmes de vol d'identité des particuliers.

Pourriel VoIP
Prolifération des appels téléphoniques pré-enregistrés, non désirés, composés automatiquement à l'aide de la voix sur protocole Internet (VoIP). Certains experts utilisent l'acronyme SPIT (pour Spam over Internet Telephony) pour s'y référer.

Vulnérabilité
L'absence ou la faiblesse d'un dispositif de protection ou d'un contrôle d'atténuation. Les vulnérabilités peuvent avoir la capacité de transformer les menaces mineures en menaces plus importantes ou en menaces plus persistantes.

Chapeau blanc
Le héros ou le bon gars, en particulier en argot informatique où il fait référence à un pirate informatique éthique qui met l'accent sur la sécurisation et la protection des systèmes informatiques. Ces personnes sont employées par des sociétés de sécurité informatique où ces professionnels sont parfois appelés des corsaires. Les équipes composées de ces personnes sont souvent appelées « Tiger teams ».

Réseau étendu (WAN)
Un réseau de réseaux locaux (LAN), qui fournit la communication et des services sur une zone géographique plus grande que celle desservie par un réseau local.

Ver
Un ver informatique est un programme conçu pour se reproduire et se propager sur un réseau en le rendant inefficace. Un ver peut être conçu pour effectuer plusieurs activités malveillantes différentes. Toutefois, le dénominateur commun est qu'un ver peut nuire à un réseau en consommant de grandes quantités de bande passante, ce qui peut potentiellement fermer le réseau. Les virus, par contre, sont plus limités ciblant les ordinateurs un à la fois. Un virus requiert également d'autres programmes pour s'exécuter et se reproduire, alors qu'un ver peut agir indépendamment des autres programmes.

Ordinateur zombie
Un ordinateur relié à Internet qui a été compromis par un pirate informatique, un virus informatique ou un cheval de Troie. En général, une machine compromise n'est qu'une des nombreuses machines d'un Botnet et sera utilisée pour effectuer des tâches malveillantes d'une sorte ou d'une autre par une commande à distance.

Pour plus d'informations sur les services et l'assurance contre les cyber-risques d'AIG, contactez-nous à cyberedge@aig.com.

CTG 11/17