Payment Card Industry (PCI) Normes en matière de sécurité des données

Glossaire, abréviations et acronymes

Terme	Définition
AAA	Protocole d'authentification, d'autorisation et de comptabilité
Acquéreur	Membre d'une association d'émetteurs de cartes bancaires initiant et maintenant des relations avec des commerçants qui acceptent des cartes de paiement
Actif	Information ou ressources de traitement de l'information d'une organisation
Administrateur de base de données	Administrateur de base de données. Personne en charge de la gestion et de l'administration de bases de données.
Adresse IP	Code numérique identifiant de manière unique un ordinateur donné sur l'Internet
Analyse cryptographique (AES)	Norme d'analyse cryptographique (*Advanced Encryption Standard*, AES). Cryptage par blocs adopté par NIST en novembre 2001. L'algorithme figure dans la FIPS PUB 197
Analyse de risque	Processus identifiant systématiquement des ressources de système précieuses et menaces à cet égard. Il quantifie l'exposition à des pertes (c'est-à-dire, à des pertes éventuelles) sur la base de fréquences et de coûts d'occurrence estimés; et (de manière optionnelle) formulant des recommandations quant à la manière d'affecter les ressources en matière de contre-mesures dans le but de minimiser l'exposition totale. Évaluation des risques.
ANSI	Institut national américain de normalisation (American National Standards Institute). Organisation privée à but non lucratif qui administre et coordonne le système de normalisation volontaire et d'évaluation de la conformité aux États-Unis
Application	Inclut tous les programmes logiciels achetés et personnalisés, ou groupes de programmes conçus pour des utilisateurs finaux, y compris des applications (Internet) internes et externes
Atteinte à la sécurité	Intrusion dans un système informatique lorsqu'une divulgation, une modification ou la destruction non autorisées de données de titulaires de carte sont soupçonnées.
Authentification	Processus de vérification de l'identité d'un sujet ou d'un processus.
Authentification à deux facteurs	Authentification nécessitant que les utilisateurs produisent deux éléments d'authentification pour accéder à un système. Les éléments d'authentification sont parfois constitués d'une chose (par exemple, une carte à puce ou des jetons matériels), ou d'une information (comme un mot de passe) en la possession de l'utilisateur. Pour accéder au système, l'utilisateur doit produire ces deux facteurs.
Autorisation	Octroi d'accès ou d'autres droits à un utilisateur, programme ou processus

Terme	Définition
Balayage de sécurité de réseau	Outil automatisé vérifiant à distance des systèmes marchands ou de prestataire de services pour déceler d'éventuelles vulnérabilités. Les tests non intrusifs impliquent le sondage des systèmes tournés vers l'extérieur, sur la base d'adresses IP tournées vers l'extérieur et établissant des rapports sur les services disponibles à l'intention d'un réseau externe (c'est-à-dire, des services disponibles sur l'Internet). Les balayages identifient les vulnérabilités des systèmes d'exploitation, des services et des dispositifs susceptibles d'être utilisés par des pirates pour cibler le réseau privé de la société.
Balayage de vulnérabilité	Balayages utilisés pour identifier les vulnérabilités des systèmes d'exploitation, des services et des dispositifs susceptibles d'être utilisés par des pirates pour cibler le réseau privé de la société.
Base de données	Format structuré d'organisation et de conservation d'informations facilement récupérables. Les tableaux et tableurs sont des exemples de base de données simples.
Changement de clé	Processus de modification des clés cryptographiques dans le but de limiter la quantité de données à crypter avec une même clé.
CIS	Centre de sécurité Internet (*Center for Internet Security*). Entreprise à but non lucratif dont la mission est d'aider les organisations à réduire le risque de perturbations commerciales et en matière de commerce électronique découlant de contrôles de sécurité techniques inadéquats.
Clé	Dans le domaine de la cryptographie, une clé est une valeur algorithmique appliquée au texte non chiffré afin de produire du texte chiffré. De manière générale, la longueur de la clé détermine le degré de difficulté du déchiffrement du texte d'un message donné.
Code de service	Numéro à trois ou quatre chiffres, figurant sur la bande magnétique, spécifiant les exigences et limitations en matière d'acceptation pour une transaction par lecture de bande magnétique.
Composants de réseau	Incluent notamment les pare-feux, commutateurs, routeurs, points d'accès sans fil, appareils de réseau et autres dispositifs de sécurité.
Composants de système	Tout composant, toute application ou tout serveur de réseau inclus dans, ou lié à l'environnement de données de titulaires de carte.
Comptabilisation	Suivi des ressources de réseau des utilisateurs.
Comptes par défaut	Compte de connexion au système prédéfini dans un système conçu pour permettre un accès initial lors de la mise en service initiale de ce système.
Connaissance partagée	Situation dans laquelle deux entités ou plus détiennent séparément des composantes clés ne permettant pas de disposer individuellement de la clé cryptographique résultante.
Console	Écran et clavier permettant l'accès au serveur ou à un ordinateur principal, ainsi que le contrôle de celui-ci, dans un environnement en réseau.
Consommateur	Personne achetant des biens ou des services, ou les deux.

Terme	Définition
Contrôle d'accès	Mécanismes limitant la disponibilité de l'information, ou les ressources de traitement de l'information, uniquement à des personnes ou applications autorisées
Contrôles correctifs	Des contrôles correctifs peuvent être envisagés lorsqu'une entité n'est pas en mesure de se conformer à une exigence telle que prévue expressément, en raison de contraintes techniques légitimes ou de contraintes commerciales consignées, mais qu'elle a suffisamment atténué les risques liés à l'exigence par la mise en œuvre d'autres contrôles. Les contrôles correctifs doivent 1) répondre à l'intention sous-jacente à, et à la rigueur de l'exigence des Normes PCI DSS indiquée initialement; 2) bloquer une tentative d'atteinte à la sécurité avec une force similaire; 3) « excéder » d'autres exigences des Normes PCI DSS (pas seulement conformément aux exigences d'autres Normes PCI DSS); et 4) être proportionnels au risque supplémentaire découlant du non-respect de l'exigence des Normes PCI DSS.
Cookies	Chaîne de données échangées entre un serveur Internet et un navigateur Internet dans le but de maintenir une session. Les cookies peuvent contenir les préférences de l'utilisateur, ainsi que des informations personnelles.
Correction d'erreurs	Intervention de réparation rapide pour un élément de programmation. Lors des bêta-tests de produit logiciel ou périodes d'essai et après la commercialisation officielle du produit, des problèmes sont détectés. Une correction d'erreur est rapidement mise à la disposition des utilisateurs.
Chiffrement	Processus de conversion d'information en une forme inintelligible sauf pour les possesseurs d'une clé cryptographique spécifique. L'utilisation du chiffrement protège l'information entre le processus de chiffrement et le processus de déchiffrement (l'inverse du chiffrement) contre la divulgation non autorisée.
Cryptographie	Discipline mathématique et informatique se rapportant à la sécurité de l'information et aux questions liées, en particulier le chiffrement et l'authentification et des applications telles que le contrôle d'accès. En matière de sécurité informatique et de réseau, un outil de contrôle d'accès et de confidentialité de l'information.

Terme	Définition
Cryptographie performante	Terme général indiquant qu'une cryptographie est extrêmement résistante à l'analyse cryptographique, ce qui signifie que, compte tenu de la méthode de cryptographie (algorithme ou protocole) utilisée, la clé cryptographique ou les données protégées ne sont pas exposées. La performance repose sur la clé cryptographique utilisée. La dimension efficace de la clé devrait correspondre à la taille de clé minimale de recommandations de performances comparables. Au nombre des références en relation avec la notion de performance minimale comparable figure la Publication spéciale NIST 800-57, août 2005 (http://csrc.nist.gov/publications/), ou d'autres correspondant aux critères suivants en matière de bits minimum de clé comparable : • 80 bits pour les systèmes basés sur une clé secrète (par exemple, TDES); • module 1 024 bits pour les algorithmes de clé publique, sur la base de la factorisation (par exemple, RSA); • 1 024 bits pour le logarithme discret (par exemple, Diffie-Hellman), avec une taille minimale de 160 bits, d'un sous-groupe important (par exemple, DSA); • 160 bits pour la cryptographie sur courbe elliptique (par exemple, ECDSA).
DES	Norme de chiffrement de données (*Data Encryption Standard*, DES). Chiffrement par bloc choisi comme Norme officielle fédérale de traitement de l'information (*Federal Information Processing Standard*, FIPS) pour les États-Unis en 1976. Remplacé par la Norme de chiffrement avancé (*Advanced Encryption Standard*, AES).
DNS	Système de nom de domaine (*Domain Name System*) ou Serveur de nom de domaine (*Domain Name Server*). Système stockant des informations associées à des noms de domaine dans une base de données distribuée sur des réseaux, tels que l'Internet.
Données d'authentification sensibles	Informations liées à la sécurité (codes/valeurs de validation de carte, données de piste complète, codes PIN et blocs PIN) utilisés pour authentifier les titulaires de carte, apparaissant sous forme de texte seul, ou sous toute autre forme non protégée. La divulgation, la modification ou la destruction de cette information pourrait compromettre la sécurité d'un dispositif cryptographique, d'un système d'information ou d'informations de titulaires de cartes, ou encore pourrait être utilisée lors d'une transaction frauduleuse.
Données de bande magnétique (Données de piste)	Données chiffrées dans la bande magnétique utilisée pour l'autorisation durant les transactions lorsque la carte est présentée. Les entités ne doivent pas conserver de données complètes de bande magnétique après l'autorisation de la transaction. De manière spécifique, après autorisation, les codes de service, données discrétionnaires/Valeurs de validation de carte/Codes et valeurs propriétaires réservées doivent être purgées; toutefois, le numéro de compte, la date d'expiration, le nom et le code de service peuvent être extraits et conservés, le cas échéant, à des fins commerciales.

Terme	Définition
Données de titulaire de carte	La bande magnétique complète ou le PAN, plus l'un ou l'autre des éléments ci-après : • nom du titulaire de carte; • date d'expiration; • code de service.
Données de transaction	Données liées à un paiement électronique
Double contrôle	Processus d'utilisation de deux entités distinctes ou plus (généralement des personnes physiques) opérant de concert pour protéger des fonctions ou informations sensibles. Les deux entités sont également responsables de la protection physique des documents impliqués dans des transactions vulnérables. Nul n'est autorisé à accéder aux documents, ou à les utiliser (par exemple, la clé cryptographique). Pour la génération manuelle de clés, le transfert, le chargement, le stockage et la récupération de données, le double contrôle nécessite de répartir la connaissance des clés entre les entités. Voir également, « répartir les connaissances ».
DSS	Normes de sécurité des données
ECC	Cryptographie sur les courbes elliptiques (*Elliptic curve cryptography*). Approche de la cryptographie à clé publique basée sur des courbes elliptiques basées sur des champs finis.
Entrée	Trafic entrant dans un réseau par le biais d'un lien de communication et du réseau du client
Environnement de données de titulaire de carte	Zone du réseau du système informatique dans laquelle sont stockées les données de titulaires de carte ou des données d'authentification à caractère sensible, ainsi que les systèmes et les segments qui joignent ou supportent directement le traitement, le stockage ou la transmission de données de titulaires de carte. Une segmentation adéquate du réseau, qui isole des systèmes stockant, traitant ou transmettant des données de titulaire de carte de ceux qui ne le font pas peut réduire le périmètre de l'environnement de données du titulaire de carte, et ainsi le périmètre de l'évaluation PCI.
Environnement de paiement de titulaire de carte	Partie du réseau contenant des données de titulaire de carte ou des données d'authentification sensibles
Épuration	Processus d'élimination de données sensibles d'un fichier, dispositif ou système; ou pour la modification de données, de sorte qu'elles deviennent inutiles lorsqu'il y est accédé lors d'une attaque.
Faisant affaire sous le nom de	Les niveaux de validation de conformité sont établis d'après le volume de transactions d'une entité « faisant affaire sous le nom de » ou d'une chaîne de boutiques (et non d'une société possédant plusieurs chaînes).
FIPS	Norme officielle fédérale de traitement de l'information (*Federal Information Processing Standard*, FIPS)

Terme	Définition
Fournisseur d'hébergement	Offres des services divers à des commerçants et autres prestataires de services. Ces services vont des plus simples aux plus complexes; du partage d'espace sur un serveur à une gamme complète d'options de « panier »; d'applications de paiement à des portails de paiement et entités de traitement; jusqu'à l'hébergement dédié d'un seul client par serveur.
FTP	Protocole de transfert de fichiers (*File Transfer Protocol*, FTP)
GPRS	General Packet Radio Service. Service mobile de données à la disposition des utilisateurs de téléphones mobiles GSM. Réputé pour une utilisation efficace d'une largeur de base limitée. Particulièrement adapté à l'envoi et à la réception de petits paquets de données, tels que des courriers électroniques et la navigation sur Internet.
GSM	Global System for Mobile Communications. Norme populaire pour les téléphones mobiles. La présence très large de la norme GSM facilite considérablement le roaming international entre opérateurs de téléphonie mobile, permettant aux abonnés d'utiliser leur téléphone dans de nombreuses régions du monde
Hôte	Principal matériel informatique sur lequel le logiciel informatique est résident
HTTP	HyperText Transfer Protocol. Protocole Internet ouvert pour le transfert ou la transmission d'informations sur le World Wide Web.
ID	Identité
Identité d'utilisateur	Une chaîne de caractères utilisée pour identifier chaque utilisateur d'un système de manière unique.
IDS/IPS	Système de détection d'intrusion (*Intrusion Detection System*)/Système de prévention d'intrusion (*Intrusion Prevention System*). Utilisé pour détecter les tentatives d'intrusion dans un réseau ou système et déclencher des alertes. Constitué de capteurs qui génèrent des événements de sécurité; d'une console de surveillance des événements et alertes, et de contrôle des capteurs; ainsi que d'un moteur central qui enregistre dans une base de données les événements détectés par les capteurs. Utilise le système de règles pour générer des alertes en réponses aux événements de sécurité détectés. Un IPS bloque en outre les tentatives d'intrusion.
IETF	Internet Engineering Task Force. Grande communauté internationale ouverte de concepteurs de réseau, opérateurs, fournisseurs et chercheurs concernés par l'évolution de l'architecture du Web et le bon fonctionnement de l'Internet Ouvert à toute personne intéressée.
Injection de commandes SQL	Type d'attaque sur un site Internet régi par une base de données. Un attaquant exécute des commandes SQL non autorisées en profitant d'un code non sécurisé sur un système lié à Internet. Les attaques par injection de commandes SQL sont utilisées pour dérober des informations provenant d'une base de données dont les données ne seraient normalement pas disponibles et/ou d'accéder aux ordinateurs hôtes d'une organisation par le biais de l'ordinateur hébergeant la base de données.
Inviolabilité	Système difficile à modifier ou à subvertir, même pour un agresseur ayant un accès physique au système.

Terme	Définition
IP	Protocole Internet. Protocole de couche de réseau contenant des informations d'adresse, ainsi que des informations de contrôle permettant le routage des paquets. Le protocole Internet est un protocole de couche de réseau dans la suite du protocole Internet.
IPSEC	Sécurité de protocole Internet (*Internet Protocol Security*, IPSEC). Norme de sécurisation des communications IP par le chiffrement et/ou l'authentification de tous les paquets IP. L'IPSEC sécurise la couche de réseau.
ISO	Organisation internationale de normalisation (International Organization for Standardization). Organisation non gouvernementale constituée d'un réseau rassemblant les instituts de normalisation de plus de 150 pays, avec un membre par pays et un secrétariat situé à Genève, en Suisse, qui coordonne le système.
ISO 8583	Norme en vigueur pour la communication entre systèmes financiers.
Jeton	Dispositif d'authentification dynamique
L2TP	Layer 2 tunneling protocol : protocole utilisé pour supporter les réseaux privés virtuels (VPN)
LAN	Réseau local d'entreprise (*Local Area Network*, LAN) : réseau informatique couvrant une petite région, souvent un bâtiment ou un groupe de bâtiments.
Logiciel malveillant	Logiciel malveillant : conçu pour infiltrer ou endommager un système informatique, sans que le propriétaire le sache, ou sans son accord.
LPAR	Partition logique : section d'un disque autre que l'une des partitions principales. Définie dans un bloc de données désigné par la partition étendue.
MAC	Code d'authentification de message (Message Authentication Code, MAC)
Menace	Situation susceptible d'entraîner la perte, la modification, l'exposition, l'indisponibilité intentionnelle ou accidentelle d'informations ou de ressources de traitement de l'information, ou encore que celles-ci seront affectées de toute autre manière au préjudice de l'organisation.
Mot de passe	Une chaîne de caractères faisant office d'authentifiant de l'utilisateur
Mot de passe par défaut	Mot de passe sur des comptes d'administration de système ou de service lorsqu'un système est expédié par le fabricant; ordinairement associé à un compte par défaut. Les comptes et mots de passe par défaut sont publiés et bien connus.
MPLS	Multi Protocol Label Switching.
NAT	Traduction d'adresse de réseau (*Network Address Translation*, NAT), également désignée « déguisement de réseau ou déguisement d'adresse IP ». Remplacement d'une adresse IP utilisée dans un réseau par une adresse IP différente connue d'un autre réseau.

Terme	Définition
NIST	Institut national des normes et de la technologie (National Institute of Standards and Technology, NIST). Agence fédérale non réglementaire de l'Administration de la technologie (Technology Administration) du ministère du commerce des États-Unis (U.S. Commerce Department). Sa mission consiste à promouvoir l'innovation et la compétitivité industrielle par la promotion de la science, les normes et la technologie dans le domaine des mesures avancées, afin de renforcer la sécurité économique et d'améliorer la qualité de vie.
Normes approuvées	Les normes approuvées sont des algorithmes normalisés (comme dans ISO et ANSI), ainsi que des normes bien connues disponibles dans le commerce (comme Blowfish), satisfaisant à la nécessité d'une cryptographie performante. Entre autres exemples de normes approuvées figurent l'AES (128 bits et plus), TDES (deux ou trois clés indépendantes), RSA (1 024 bits) et ElGamal (1 024 bits)
NTP	Protocole de synchronisation des horloges de systèmes informatiques de réseaux de données à commutation par paquets à latence variable
Numéro de compte	Le numéro de carte de paiement (de crédit ou de débit) qui identifie l'émetteur et le compte spécifique du titulaire de carte. Également dénommé numéro de compte primaire (*Primary Account Number*, PAN)
OWASP	Open Web Application Security Project (voir http://www.owasp.org)
PAD	Assembleur-désassembleur de paquets. Dispositif de communication formatant les données sortantes et les données de bande provenant des paquets entrants. Dans le domaine de la cryptographie, le PAD unique est un algorithme de chiffrement avec un texte combiné à une clé aléatoire ou *« PAD »* aussi longue que le texte seul et utilisée une seule fois. En outre, si la clé est réellement aléatoire, si elle n'est jamais réutilisée et si elle est tenue secrète, le PAD unique est inviolable.
PAN	Le numéro de compte principal (*Primary Account Number*, PAN) est le numéro de carte de paiement (de crédit ou de débit) qui identifie l'émetteur et le compte spécifique du titulaire de carte. Également désigné comme Numéro de compte.
Pare-feu	Matériel informatique, logiciel, ou toute combinaison des deux protégeant les ressources d'un réseau contre des intrusions provenant d'autres réseaux. De manière générale, une entreprise équipée d'un réseau intranet permettant à ses collaborateurs d'accéder à Internet doit être équipée d'un pare-feu pour empêcher des intervenants extérieurs d'accéder à des ressources internes en données privées.
PAT	Traduction d'adresse de port (*Port Address Translation*, PAT). Comporte un dispositif de traduction d'adresse de réseau (Network Address Translation, NAT) qui traduit les connexions par protocole de contrôle de transmission (Transmission Control Protocol, TCP) ou Protocole datagramme d'utilisateur (User Datagram Protocol, UDP) vers un hôte et un port sur un réseau extérieur, vers un hôte et un port sur un réseau intérieur.
PCI	Industrie des cartes de paiement (*Payment Card Industry*)
Pénétration	Tentative couronnée de succès pour contourner les mécanismes de sécurité et accéder au système informatique.

Terme	Définition
PIN	Code d'identification personnel ou code PIN (*Personal Identification Number*).
Point de vente	Point de vente
Politique	Règles à l'échelle de l'organisation régissant l'utilisation acceptable des ressources informatiques et les pratiques en matière de sécurité, et guidant le développement des procédures opérationnelles.
Politique en matière de sécurité	Ensemble de lois, règles et pratiques régissant la manière dont une organisation gère, protège et distribue des informations sensibles.
Prestataire de services	Entité commerciale autre qu'un membre d'une marque de carte de paiement ou un marchand directement impliqué dans le traitement, le stockage, la transmission et la commutation, ou les données de transmission ou informations de titulaire de carte, ou les deux. Inclut également des sociétés fournissant des services à des commerçants, prestataires de services ou membres contrôlant, ou susceptibles d'impacter, la sécurité des données des titulaires de carte. Entre autres exemples figurent des fournisseurs de services gérés qui mettent à disposition des pare-feux, IDS et autres services, ainsi que des fournisseurs d'hébergement et d'autres entités. Des entités telles que des sociétés de télécommunications fournissant uniquement des liens de communication sans accès à la couche application du lien de communication sont exclues.
Procédure	Narration descriptive afférente à une politique. La procédure est le « comment faire » d'une politique et décrit la manière dont celle-ci est mise en œuvre.
Programme antivirus	Programmes capables de détecter, de supprimer et d'assurer une protection contre diverses formes de codes ou de logiciels malveillants, y compris des virus, vers, chevaux de Troie, logiciels espions et publicitaires.
Protocole	Méthode de communication convenue utilisée dans le cadre des réseaux. Spécifications décrivant les règles et procédures auxquelles les produits informatiques doivent se conformer pour exécuter leurs activités sur un réseau.
PVV	Valeur de vérification du numéro d'identification personnel (PIN Verification Value). Codé sur la piste magnétique de la carte de paiement.
RADIUS	Remote Authentication and Dial-In User Service : système d'authentification et comptable. Vérifie si des informations telles que le nom d'utilisateur et le mot de passe communiqués au serveur RADIUS sont exactes, puis autorise l'accès au système.
Récolte de comptes	Processus d'identification comptes d'utilisateurs existants par tâtonnements. [Remarque : le fait de fournir des informations excessives dans les messages d'erreurs peut divulguer suffisamment d'éléments pour faciliter les efforts de pénétration ou de « récolte » d'un attaquant, ou encore pour compromettre la sécurité du système.]
Registre de vérification	Enregistrement chronologique des activités du système. Constitue une piste suffisante pour permettre la reconstruction, l'étude et l'examen d'une séquence d'environnements et d'activités entourant ou conduisant à une opération ou procédure, ou à un événement dans une transaction, du début jusqu'aux résultats finaux. Parfois désigné spécifiquement « piste de vérification en matière de sécurité ».

Terme	Définition
Réseau	Deux ordinateurs ou plus, connectés ensemble, pour partager des ressources
Réseau public	Réseau mis en place et exploité par un fournisseur de services de télécommunication ou une société privée reconnue, dans le but spécifique de fournir au public des services de transmission de données. Les données doivent être cryptées lors de leur transmission sur les réseaux publics, car il n'est pas rare que des pirates interceptent, modifient et/ou détournent aisément des données en cours de transit. Entre autres exemples de réseaux publics intéressant les Normes PCI en matière de sécurité des données (DSS) figurent l'Internet, le GPRS et le GSM.
Responsable de la sécurité	Personne principalement responsable des affaires liées à la sécurité au sein d'une organisation.
RFC	Appel à commentaires (*Request For Comments*, RFC)
Routeur	Matériel ou logiciel informatique connectant deux réseaux ou plus. Fait office de dispositif de triage et d'interprétation par l'examen d'adresses et la transmission d'éléments d'information à des destinations adéquates. Les routeurs de logiciel sont parfois désignés sous le nom de « portail ».
RSA	Algorithme pour les cryptages de clé publique décrits en 1977 par Ron Rivest, Adi Shamir et Len Adleman, du Massachusetts Institute of Technology (MIT). L'acronyme RSA est constitué des initiales de leurs noms de famille.
SANS	SysAdmin, Audit, Network, Security Institute (voir www.sans.org)
Sauvegarde	Copie de données dupliquées réalisée à des fins d'archivage, ou aux fins de protection contre des dommages ou leur perte éventuelle
Sécurité de l'information	Protection de l'information pour garantir la confidentialité, l'intégrité et la disponibilité
Séparation des obligations	Pratique consistant à répartir les diverses étapes d'une fonction entre diverses personnes, afin d'éviter qu'une personne seule ne puisse subvertir l'ensemble du processus.
Serveur	Ordinateur fournissant un service à d'autres ordinateurs, tel que le traitement de communications, le stockage de fichiers ou l'accès à une installation d'impression. Les serveurs incluent notamment l'Internet, les bases de données, l'authentification, les DNS, serveurs courrier, serveurs mandataire et NTP.
SHA	Algorithme de chiffrement irréversible (*Secure Hash Algorithm*). Une famille ou un ensemble de fonctions de chiffrement cryptographique liées. SHA-1 est la fonction la plus couramment utilisée. L'utilisation d'une valeur salée (« *salt value* ») unique réduit les risques de collision de valeur chiffrée.
SNMP	Protocole de gestion de réseau simple (*Simple Network Management Protocol*, SNMP). Compatible avec la surveillance de dispositifs liés au réseau en liaison avec toutes situations requérant une attention administrative.
Sortie	Trafic sortant d'un réseau par le biais d'un lien de communication vers le réseau du client

Terme	Définition
SQL	Langage relationnel SQL (Structured (English) Query Language, SQL). Langage informatique utilisé pour créer, modifier ou récupérer des données provenant de systèmes de gestion de base de données relationnelle.
SSH	Secure Shell : suite de protocole fournissant un chiffrement pour des services de réseau tels que la connexion à distance ou le transfert de fichiers à distance.
SSID	Service Set Identifier : dénomination des réseaux WiFi ou IEEE 802.11 sans fil.
SSL	Protocole SSL (Secure Sockets Layer) : norme sectorielle établie qui chiffre le canal entre un navigateur ou serveur Internet, afin de garantir le caractère privé et la fiabilité des données transmises sur ce canal.
Surveillance	Utilisation d'un système supervisant en permanence un réseau informatique, y compris dans le cas des systèmes lents et défaillants, et qui informe l'utilisateur en cas de rupture d'alimentation ou du déclenchement d'autres alarmes.
Système d'information	Ensemble discret de ressources en données structurées organisées pour la collecte, le traitement, la maintenance, l'utilisation, le partage, la diffusion ou l'élimination de l'information
Systèmes de détection d'intrusion	Voir IDS
TACACS	Système de contrôle d'accès de contrôleur d'accès de terminal (*Terminal Access Controller Access Control System*, TACACS) : protocole d'authentification à distance.
TCP	Programme de gestion de terminaux (*Transmission Control Protocol*, TCP)
TDES	Triple Data Encryption Standard, également désigné 3DES. Cryptage par bloc créé à partir du chiffrement DES en l'utilisant trois fois.
TELNET	Protocole de réseau téléphonique. Généralement utilisé pour mettre à disposition des sessions de connexion par ligne de commande orientées utilisateur, entre les hôtes sur Internet. Programme initialement conçu pour émuler un terminal unique lié à l'autre ordinateur.
Test de pénétration	Test de sécurité d'un système ou réseau informatique mis en œuvre dans le but de rechercher des vulnérabilités qu'un pirate pourrait exploiter. Par delà la détection des vulnérabilités, ce test peut inclure des tentatives de pénétration effective. L'objectif du test de pénétration est de détecter et d'identifier les vulnérabilités, ainsi que de suggérer des améliorations possibles de la sécurité.
Titulaire de carte	Consommateur auquel une carte est délivrée ou personne autorisée à utiliser la carte
TLS	Sécurité de couche transport (*Transport Layer Security*, TLS) : conçue dans le but d'assurer le secret et l'intégrité des données entre deux applications de communication. Le protocole TLS a remplace le protocole SSL.
Troncature	Pratique de suppression du segment données. D'ordinaire, lorsque les numéros de compte sont tronqués, les 12 premiers chiffres sont supprimés, seuls les 4 derniers demeurent apparents.

Terme	Définition
UDP	Protocole datagramme d'utilisateur (*User Datagram Protocol*, UDP)
Usurpation d'IP	Technique utilisée par l'auteur d'une intrusion pour accéder aux ordinateurs sans autorisation. Le pirate envoie des messages trompeurs à un ordinateur, avec une adresse IP indiquant que le message provient d'un hôte de confiance.
Utilisateurs non-clients	Toute personne, à l'exclusion de clients consommateurs, accédant à des systèmes, y compris notamment des employés, des administrateurs et des tiers
Valeur ou code de validation de carte	L'élément données sur la bande magnétique d'une carte qui fait appel à un processus cryptographique pour protéger l'intégrité des données figurant sur la bande, et révèle toute altération ou contrefaçon. Désigné par les acronymes CAV, CVC, CVV ou CSC, en fonction de la marque de la carte de paiement. La liste ci-après inclut les termes pour chaque marque de carte : • **CAV :** (*Card Authentication Value*) valeur d'authentification de carte (cartes de paiement JCB); • **CVC :** (*Card Validation Code*) code de validation de carte (cartes de paiement MasterCard); • **CVV :** (*Card Verification Value*) valeur de vérification de carte (cartes de paiement Visa et Discover); • **CSC :** (*Card Security Code*) code de sécurité de carte (American Express). *Remarque : le deuxième type de valeur ou de code de validation de carte est une valeur à trois chiffres imprimée à droite du numéro de la carte de crédit, dans l'espace signature au dos de la carte. Dans le cas des cartes American Express, le code est un numéro à quatre chiffres imprimé (et non en relief) au-dessus du numéro de carte, au recto de toutes les cartes de paiement. Le code est uniquement associé à chaque pièce de plastique individuelle et lie le numéro de compte de la carte à ce morceau de plastique. Les éléments ci-après fournissent un aperçu :* • **CID :** (*Card Identification Number*) numéro d'identification de carte (cartes de paiement American Express et Discover); • **CAV2 :** (*Card Authentication Value 2*) valeur d'authentification de carte 2 (cartes de paiement JCB); • **CVC2 :** (*Card Validation Code 2*) code de validation de carte 2 (cartes de paiement MasterCard); • **CVV2 :** (*Card Verification Value 2*) valeur de vérification de carte 2 (cartes de paiement Visa).
Virus	Programme ou chaîne de codes susceptible de se reproduire elle-même, ou de causer une modification ou la destruction d'un logiciel ou de données.
VPN	Réseau privé virtuel (*Virtual Private Network*, VPN). Réseau privé mis en place sur un réseau public.
Vulnérabilité	Faiblesse des procédures de sécurité d'un système, de la conception d'un système, de son fonctionnement ou de contrôles internes susceptibles d'être exploités dans le but de contrevenir à la politique en matière de sécurité

Terme	Définition
WEP	Wired Equivalent Privacy : protocole destiné à prévenir les écoutes accidentelles et destiné à assurer une confidentialité comparable à celle du réseau câblé de type traditionnel. N'assure pas une sécurité suffisante contre les écoutes intentionnelles (par exemple, l'analyse cryptographique).
WPA	WiFi Protected Access (WPA et WPA2) : protocole de sécurité pour les réseaux sans fil (WiFi). Élaboré en réponse à un certain nombre de faiblesses graves contenues dans le protocole WEP.
XSS	Cross-Site Scripting (XSS ou CSS). Type de vulnérabilité en matière de sécurité généralement contenu dans les applications Internet. Peut être utilisé par un attaquant pour obtenir un privilège élevé d'accès à un contenu de page, des cookies de session et divers autres objets à caractère sensible.
Zone d'accueil	Zone d'accueil (« zone démilitarisée », ou « zone DMZ »). Réseau ajouté entre un réseau privé et un réseau public, afin de constituer une couche de sécurité supplémentaire.