Glossaire Cyber & Data

A

Advanced Persistent Threat (APT)

Attaque ciblée, c'est-à-dire dirigée contre une structure en particulier, basée sur des mécanismes plus complexes que les attaques à grandes échelles type spamming (failles 0-day, vulnérabilités spécifiques du système d'information, etc.). Elle est qualifiée de persistante car elle va en général perdurer jusqu'à ce que son objectif soit atteint. En général, ces attaques sont précédées d'une longue période de préparation, à la fois technique et relevant de l'ingénierie sociale*.

Amendes et pénalités PCI

Amendes et pénalités que les banques infligent en cas de non-conformité aux normes PCI DSS*. Elles peuvent aller jusqu'à 100.000 dollars par mois.

Application service provider (ASP)

Entreprise qui fournit des logiciels ou des services informatiques à ses clients au travers d'un réseau et non en les installant sur leurs propres machines. Notion remplacée aujourd'hui de plus en plus par celle de Software as a Service (SaaS*).

Authentification

Processus de vérification de l'identité (ou d'autres attributs) d'un individu. Peut être simple ou multi-facteurs, c'est-à-dire faire appel à plusieurs méthodes simultanément (login et mot de passe pour se connecter + code envoyé par sms, par exemple, ou mot de passe + empreinte rétinienne).

B

Bot

Ordinateur connecté à internet ou à un réseau local, qui a été compromis via un malware* qui permet sa prise de contrôle à distance par un hacker*.

Botnet

Série d'ordinateurs compromis par un malware et contrôlés par le biais d'un réseau. Utilisé notamment dans les attaques DDoS.

Brute force

Cyber-attaque « par tâtonnement », qui vise à décoder des données cryptées en essayant toutes les combinaisons possibles ou à forcer l'accès à un système d'information jusqu'à trouver une faille qui permet d'entrer. Cette méthode prend beaucoup de temps et peut être rendue beaucoup moins efficaces par des mesures de sécurité assez basiques.

C

Cheval de Troie – malware*

Conçu pour être introduit dans un système informatique et, une fois dedans, s'exécuter pour y voler ensuite des données ou endommager l'ordinateur.

Cloud computing / SaaS, PaaS, IaaS

Système dans laquelle une solution et/ou une infrastructure informatique est gérée par des serveurs auxquels les usagers se connectent via un réseau / internet. L'ordinateur de bureau ou portable, le téléphone mobile, la tablette et autres objets connectés deviennent des points d'accès pour exécuter des applications ou consulter des données qui sont hébergées sur les serveurs au lieu d'être localisés sur le poste de l'utilisateur (approche de dématérialisation des systèmes informatiques).

Software as a Service (SAAS) : modèle de cloud computing suivant lequel une application est construite sur une infrastructure cloud et accessible via internet aux utilisateurs finaux (webmails par exemple). Le logiciel est utilisé comme s'il s'agissait d'un service : le client paye un abonnement sans s'occuper de la maintenance et peut accéder à l'interface de n'importe où avec un outil connecté à internet.

Platform as a Service (PAAS) : modèle de cloud computing suivant lequel la plateforme (système d'exploitation et outils) est gérée par le fournisseur via le cloud, les applications étant de la responsabilité du client.

Infrastructure as a Service (IaaS) : modèle de cloud computing suivant lequel la plateforme (système d'exploitation et outils) et les applications sont gérées par le fournisseur via le cloud. C'est le stade le plus abouti de la dématérialisation des systèmes informatiques.

Conseil des normes de sécurité PCI (Payment Card Industry)

Organe dirigeant du PCI. Le Conseil des normes de sécurité PCI (PCI SSC) a été formé en septembre 2006 par American Express, Discover Financial Services, Japan Credit Bureau, MasterCard Worldwide et Visa International. Le site du Conseil des normes de sécurité PCI répertorie environ 700 membres / adhérents.

Cryptographie

Méthodes consistant à protéger des informations en les convertissant dans un format illisible pour tout individu ne disposant pas de la clé de décryptage. Il existe différentes formes de

Glossaire Cyber & Data

chiffrement, le format le plus largement répandu étant le PGP (Pretty Good Privacy).

Cyber-fraude

Méthode consistant, pour un cyber-pirate, à induire en erreur un individu, le plus souvent via usurpation d'identité, pour qu'il lui livre des données sensibles ou lui transfère des fonds, en utilisant différentes techniques comme l'intrusion dans un système d'information, le harponnage*, le hameçonnage* ou le piratage de messagerie électronique.

D

Data center

Un data center est une installation qui permet à une entreprise soit de stocker ses propres données, soit d'offrir à ses clients des services de stockage et d'hébergement. Sa taille peut varier, d'une seule baie à une batterie de serveurs (des centaines de rails de serveurs dans une salle dédiée). Il est en principe construit sur la base d'alimentations et systèmes de communication redondants, de systèmes de contrôles de l'environnement (climatisation, prévention incendie, etc.) et de dispositifs de sécurité (surveillance, alarme…).

DDoS (Distributed Denial of Service)

Type de cyber-attaque pendant laquelle des systèmes corrompus (les bots*) sont utilisés pour inonder une cible de trafic réseau, causant ainsi la mise hors ligne du réseau ou du site visé.

Données à caractère personnel / Personally identifiable information

Toutes les informations qui permettent d'identifier une personne, en elles-mêmes ou par recoupement avec d'autres données ; elles peuvent notamment comprendre les données médicales (statut médical, soins, dossier médical, paiement des soins), les données bancaires (IBAN / RIB, données de connexion…) et cartes de crédit (numéro de CB, nom du titulaire, date d'expiration, code de sécurité), les documents d'identification (carte d'identité, permis de conduire, passeport, sécurité sociale), etc.

E

Evaluations PCI (conformité)

Audit de validation de la conformité d'une entreprise avec la norme PCI DSS* applicable. Dans certaines circonstances et pour de faibles volumes, un principe d'auto-évaluations est possible ; dans les autres cas, des audits complets sont exigées, menés par un organisme certifié (QSA, qualified security assessor). Liste des QSA disponible ici :

www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

Evaluations PCI (frais)

Somme due par une entreprise ayant subi une violation de données* carte de paiement, qui peut inclure les frais de réémission de la carte et les transactions frauduleuses non remboursables effectuées avec les cartes volées. Ces montants sont en général contractuellement mis à la charge de l'entreprise qui a subi l'incident par les contrats de service aux commerçants et les contrats de traitement des paiements.

F

Faille 0-Day

Exploit qui tire parti d'une faille de sécurité le jour même où la vulnérabilité est connue du public. Ces exploits sont en principe bloqués ultérieurement par des patchs de sécurité/des mises à jour fournies par l'éditeur du logiciel.

FTP (File Transfer Protocol)

Protocole de transfert de fichiers via Internet.

Forensics

Application de techniques d'enquête et d'analyse pour rassembler et préserver des preuves sur un appareil informatique (en principe afin de les présenter devant un tribunal). Il s'agit de la première mesure à mettre en place pour identifier la taille, l'ampleur et la cause d'une violation de donnée – c'est un peu la médecine légale de la cyber-sécurité.

H

Hacker

Le hacker est un cyber-pirate, un individu qui cherche à contourner les protections d'un logiciel, d'un site internet ou d'un système d'information afin de s'y introduire et/ou d'accéder aux données qu'il contient. Le « Black hat » (cyber-pirate animé d'intentions malveillantes) s'oppose traditionnellement aux « White hats » ou « Ethical hackers », dont le but est de sensibiliser individus, entreprises et administrations aux problématiques de cyber-sécurité sans les exploiter à des fins malveillantes.

Hacktivisme

Terme faisant référence aux motivations de certains cas de piratage, politiques ou sociales, plutôt que purement financières (les attaques d'Anonymous en sont un bon exemple).

Hameçonnage / phishing

Technique par laquelle des cyber-pirates se font passer pour des interlocuteurs de confiance

(grandes sociétés, organismes financiers) familiers de leurs cibles, et leur demandent par email des informations confidentielles (type mots de passe, numéros de comptes bancaires, etc) ou des transferts de fonds, ou encore les incitent à se connecter sur une page web corrompue. C'est une méthode qui relève de l'ingénierie sociale* (exploitation d'une faille humaine plutôt que technique).

Les campagnes de phishing sont en général lancées à très grande échelle, et si la majorité des destinataires de l'email frauduleux ne se sentiront pas concernés (car pas clients de la banque choisie, par exemple), certains iront quand même jusqu'à lire le mail et ouvrir la pièce jointe / cliquer sur le lien.

Se rattachent aussi au hameçonnage le spear-phishing, ou harponnage (se concentrer sur un seul utilisateur ou service) ou le whale-phishing / hameçonnage ciblé (se concentrer sur des personnes à haut revenu).

Hébergement

Allocation d'espace sur un serveur pour stocker et mettre à disposition des applications, données ou sites web conçus et gérés par des tiers, et qui permet notamment aux entreprise une meilleure maîtrise des coûts et niveaux de service et davantage de flexibilité. Traditionnellement, il existe plusieurs types d'offres :

- Les hébergeurs sur serveurs dédiés proposent à leurs clients une infrastructure machine dédiée avec des prestations annexes comme la TMA (tierce maintenance applicative), et peuvent gérer pour le compte du client les évolutions de l'infrastructure logicielle et les mises à jour de versions.
- Les hébergeurs sur serveurs mutualisés ciblent plutôt les petites structures en en exploitant plusieurs sites client sur une même machine, ce qui permet une offre moins onéreuse.
- Les prestataires de cloud public proposent des offres qui reposent sur des plates-formes d'instances de serveur virtualisées, accessibles et gérables 100% en ligne. Elles permettent de mutualiser une ou plusieurs grappes de serveurs entre plusieurs clients (un client pouvant ainsi utiliser à la demande les ressources machines des grappe en fonction de ses besoins du moment), et non plus un serveur unique.

I

Ingénierie sociale

Manipulation d'individus à des fins d'obtenir des informations sécurisées ou des données confidentielles en les incitant à la confiance, souvent par l'usurpation d'identité.

Intrusion

Entrée dans un système d'information par un individu qui n'y est pas autorisé, que ce soit par « Brute force* » ou en usurpant l'identité d'un utilisateur habituel du système. Il est possible d'identifier ce type d'attaque à l'aide d'un outil de détection des intrusions (IDS).

K

Keylogger

Malware* utilisé pour espionner les données de frappe sur un ordinateur. Ce logiciel est aussi susceptible de crypter ces données, et d'en cacher la transmission à un hacker*.

L

Location d'espace

Pratique consistant à louant de l'espace, des systèmes de refroidissement, de l'électricité et de la bande passante auprès d'un hébergeur / data center*, ce qui permet à une entreprise de placer ses propres ressources (serveurs, stockage) dans un environnement de qualité, géré par ledit hébergeur (par exemple des cages sécurisées).

M

Malware

Abréviation de « malicious software », logiciel malveillant généralement conçu pour endommager, espionner ou perturber un système (virus*, cheval de Troie*, etc.).

Micrologiciel

Logiciel intégré dans du matériel informatique / électronique afin que ce matériel puisse fonctionner. L'exploitation d'une faille de sécurité présente dans un micrologiciel permet de s'introduire dans un système d'information via une « backdoor ».

N

Normes PCI DSS

Établies par le Conseil des normes de sécurité PCI*, les normes PCI DSS définissent le niveau minimum de sécurité exigé d'une organisation qui traite des transactions de carte de paiement (4 niveaux suivant le volume annuel de transactions). Informations supplémentaires

Glossaire Cyber & Data

disponibles ici :

www.pcisecuritystandards.org/

Notification

Dans la terminologie de la cyber-assurance, la notification fait référence au fait de prévenir, en cas d'incident de cyber-sécurité, les individus dont les données personnelles* ont pu être compromises. La réglementation applicable en cas de violation de données* personnelles* varie significativement selon les pays, mais de manière générale elle tend partout vers plus de protection des individus.

P

Paquet

Unité de données transférée sur un réseau.

Pare-feu

Système utilisé pour empêcher l'accès non autorisé à ou depuis un réseau privé. Les pare-feu peuvent être mis en place à la fois via des solutions matérielles et logicielles.

Piratage téléphonique

Utilisation d'un terminal pour détourner un système téléphonique. En général, le piratage téléphonique est employé pour passer des appels gratuits ou pour que les appels soient facturés sur un compte différent. Il s'agit de l'une des plus anciennes formes de « hameçonnage* » (le phreaking).

Plan de réponse à incident

Plan mis en place par une entreprise ou une administration afin de gérer les suites d'un incident de cyber-sécurité : il comprend en principe la définition de ce qu'est un incident, les process à suivre et rôles de chacun, ainsi que les coordonnées des interlocuteurs internes et externes à contacter.

PDV (Point de vente) / POS (Point of sale)

Collecte de données et d'informations de paiement dans un lieu de vente physique (magasin). Peut également désigner la plateforme logicielle utilisée pour collecter et/ou transmettre ces informations.

R

Ramscraping

Technique utilisée par certains malwares* afin d'extraire les informations carte de paiement de la mémoire d'une machine avant qu'elles ne soient cryptées.

Ransomware

Type de malware* qui restreint l'accès au système de l'ordinateur qu'il infecte et exige qu'une rançon soit payée au(x) créateur(s) du malware pour lever la restriction.

S

Sauvegardes

Copie périodique des données, infrastructures ou autres informations sensibles/critiques d'une entreprise, en général hors site / géographiquement éloignée.

SCADA & Systèmes de contrôles de process industriel

Systèmes de supervision / Process control systems (PCS) : technique industrielle de suivi et de pilotage informatique de procédés de fabrication automatisés. La supervision concerne l'acquisition de données (mesures, alarmes, retour d'état de fonctionnement, etc.) et la gestion de paramètres de commande des processus généralement confiés à des automates programmables, afin de permettre la prise de décision centralisée / à distance.

Distributed control systems (DCS) / Système numérique de contrôle-commande (SNCC) : système de contrôle d'un procédé industriel doté d'une interface homme-machine pour la supervision ainsi que d''un réseau de communication numérique. Il est basé sur l'installation de terminaux à chaque point du process, tous reliés à une console centrale qui rassemble et distribue les instructions.

Supervisory control and data acquisition software (SCADA) / Système de contrôle et d'acquisition de données : système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures à distance au sein d'installations techniques, grâce à des instruments de mesures disséminés partout dans le système, la collecte et le traitement des informations étant centralisée. Initialement centrés sur la récolte d'informations, les SCADA sont aujourd'hui de plus en plus capable d'intégrer des fonctions de contrôle des process, ce qui les rapproche des SNCC.

SSL (Secure Sockets Layer)

Le protocole SSL permet de transmettre des données confidentielles par internet en utilisant des systèmes de cryptage à deux clés (très utilisé en particulier pour les transactions financières). Les navigateurs web indiquent qu'une connexion est protégée par protocole SSL en affichant un cadenas ou un certificat de sécurité près du champ URL.

Glossaire Cyber & Data

Spoofing — Technique visant à tromper un terminal, un logiciel ou un système d'information, par exemple en contrefaisant un numéro de téléphone ou une adresse IP.

Spyware — Logiciel qui collecte les informations d'un système d'information ou d'une interface web à l'insu de l'utilisateur, souvent à des fins publicitaires ou d'espionnage industriel.

T

Test d'intrusion (pen test) — Méthode d'évaluation de la sécurité d'un système d'information via la simulation de cyber-attaques en conditions réelles, afin d'identifier les failles, vulnérabilités*, mauvaises pratiques, etc.

V

Ver — Programme ou algorithme qui se réplique sur un réseau informatique.

Violation de données — Incident de sécurité au cours duquel des données sensibles, protégées ou confidentielles sont copiées, transmises, consultées, volées ou utilisées par une personne qui n'y est pas autorisée. Les violations de données sont soumises à des régimes et définitions spécifiques qui varient significativement selon les pays.

Virus — Programme ou élément de code malveillant installé sur un ordinateur par un utilisateur sans le savoir.

Vulnérabilité — Faille exploitable dans la structure d'un logiciel ou d'un système.

Pourquoi mon client a-t-il besoin d'une cyber-assurance ?

J'ai souscrit un avenant à ma police RC, est-ce suffisant ?
En général, cela ne suffit pas, car la plupart des avenants cyber disponibles sur le marché proposent une couverture très limitée tant sur le montant que sur le périmètre des garanties.

Je ne constitue pas une cible comme Sony, Orange ou Ashley Madison. Pourquoi m'inquiéter ?
Les grandes entreprises font la une des journaux. Pas les petites. En matière d'incidents de cyber-sécurité, la question à se poser est « quand » l'attaque arrivera-t-elle, pas « si » elle arrivera. Il existe un marché noir où les données sont échangées avec une très grande facilité : se créer une identité virtuelle, aujourd'hui, coûte moins de 250 dollars. Sony ou Orange sont des entreprises qui ont des services entiers dédiés à l'analyse et à la gestion de leurs risques, en particulier en cas de cyber-incident, et leurs systèmes et données font quand même l'objet d'attaques. Les plus petites entreprises, qui n'ont pas les mêmes ressources, sont des proies plus faciles et rentables pour les hackers.

Pourquoi la protection technique assurée par mon service informatique n'est-elle pas suffisante ?
Lorsqu'on est en position de défense, on est toujours en retard sur ses attaquants, et les hackers font preuve d'une imagination sans limite quand il s'agit de trouver des failles leur permettant d'entrer dans le système d'information d'une entreprise : une simple erreur technique, par exemple ne pas mettre à jour un logiciel, ne pas paramétrer les bonnes procédures d'authentification, perdre un ordinateur portable non crypté, etc. peut ouvrir la porte à un incident.

Ai-je besoin de cette couverture si je ne stocke pas d'informations client sur mon réseau ?
Oui. Vous ne stockez peut-être pas de données clients, mais vous y avez accès, et vous pouvez être responsable de leur traitement et de leur confidentialité même lorsque vous sous-traiter le stockage ou l'hébergement à des tiers. Par ailleurs, les données qui concernent vos employés sont en général bien stockées sur vos systèmes, et leur compromission vous impose le même type d'obligations qu'en cas de violation des données de vos clients Vous pouvez provoquer une violation des données de votre client, et donc violer un contrat. Les informations de l'entreprise sont également couvertes dans le cadre d'une police d'assurance contre la violation de la confidentialité/des données. Les données relatives aux employés sont également une responsabilité.

Je sous-traite le paiement par cartes de crédit à un tiers. Je n'ai donc pas d'exposition par rapport aux cartes de paiement ?
Les normes PCI DSS ont vocation à s'appliquer à l'ensemble des organisations et commerçants qui acceptent, transmettent, ou stockent des données cartes bancaires, indépendamment du volume ou du nombre de transactions. Le simple fait de faire appel à un sous-traitant ne dispense donc pas l'entreprise de s'y conformer pas la conformité de l'entreprise aux normes PCI DSS, et ce d'autant plus que la CNIL elle-même encourage les entreprises à respecter ce standard, qui permet de réduire l'exposition au risque.

Si les données personnelles qui m'ont été confiées sont stockées dans le cloud, la responsabilité incombe au fournisseur du cloud ?
Non, vous restez responsable de traitement des données personnelles qui vous sont confiées même lorsque vous en sous-traitez l'hébergement. Cela implique qu'en cas de compromission desdites données, vous aurez la charge de notifier les individus et le régulateur, et devrez prendre en charge leurs éventuelles réclamations ou sanctions. Si votre contrat d'hébergement vous permet de vous retourner ensuite contre votre sous-traitant, cela pourra limiter votre exposition, mais la plupart de ces contrats ne prévoit pas de maintien des recours.

Typologie des risques Cyber

Attaques commanditées par un Etat	Un groupe employé par le gouvernement d'un Etat (Chine, Russie, Armée électronique syrienne…)
Script Kiddies	Individu ou groupe (souvent inexpérimenté), agissant de son propre chef : faire tomber le réseau de son école « pour rire », défacer des sites internet dans l'espoir d'impressionner quelqu'un, ou tout simplement recourir à des malwares ou des botnets préfabriqués, sans valeur ajoutée.
Hacktivisme	Attaques réalisées pour attirer l'attention sur, ou gêner le soutien à, une cause identifiée (par exemple la liberté d'expression, un projet de loi…) : Anonymous, Lulzsec, affaire WikiLeaks.
Crime organisé	Groupes de criminels menant des activités d'extorsion de fonds en ligne ou engagés pour mener une attaque ciblée, concepteurs / producteurs de ransomware, voleurs de données revendues ensuite au marché noir…
Menaces internes	Employés, utilisateurs privilégiés ou partenaires d'une entreprise (négligence et malveillance).
Cyber-terrorisme	Attaques menées à seule fin de provoquer la peur ou la panique, pour des motivations idéologiques ou politiques, qui peuvent être associées à un groupe terroriste connu (Daesh).
Divulgation accidentelle	Négligence ou imprudence d'employés ou de partenaires de l'entreprise, qui compromet la confidentialité de données personnelles ou confidentielles qu'elle détient.
Failles 0-day	Exploiter la vulnérabilité d'un logiciel dès qu'elle est détectée et avant qu'elle ne soit corrigée.
Ingénierie sociale	Attaques d'hameçonnage.
Perte de terminaux	Conséquences plus sévères lorsque (comme très souvent) le contenu n'est pas crypté – le cryptage est un processus d'encodage des messages ou des informations, qui permet de s'assurer que seules les parties autorisées puissent y avoir accès. (ordinateur, téléphone tablette, PDA, clé USB, DVD…)
Malwares	Abréviation pour « malicious software », c'est-à-dire un logiciel malveillant destiné à endommager ou perturber un système (virus, cheval de Troie). Le virus, par exemple, est un programme ou élément de code malveillant qui est installé par un utilisateur sur son ordinateur involontairement (ouverture d'une pièce jointe à un mail de phishing par exemple).
Botnets	Une série d'ordinateurs compromis par un malware qui permet leur prise de contrôle à distance par le biais d'un réseau. Utilisés par exemple dans les attaques DDoS pour lancer un très grand nombre de requêtes simultanées.
Ransomware	Un type de malware particulier qui restreint l'accès au système de l'ordinateur qu'il infecte ou aux données qui y sont stockées, et exige qu'une rançon soit payée au(x) créateur(s) du malware pour lever la restriction.
Mauvaise gestion du parc informatique	Par exemple, ne pas s'assurer du nettoyage complet des appareils que l'on jette ou que l'on rend après utilisation. (ordinateur, téléphone tablette, PDA, clé USB, DVD…)