Comment réagir en cas d'attaque informatique ?

Chaque année, le CLUSIF (Club de La Sécurité de l'Information Français) livre une rétrospective des « cybercrimes » majeurs recensés au cours de l'année précédente dans le monde[1]*. Ce panorama des attaques informatiques montre une tendance en évolution depuis quelques années : les pirates informatiques s'intéressent moins à la célébrité qu'aux perspectives de soutirer de l'argent à leurs victimes ou d'en gagner à leurs dépends.*
C'est pour cette raison que les entreprises représentent aujourd'hui une cible de choix. Les PME, plus nombreuses et bien moins outillées que les grands comptes, intéressent particulièrement les cybercriminels.

Les conséquences d'une attaque informatique peuvent être minimisées, à condition de prendre les bonnes mesures et d'agir vite…car en matière de cybercriminalité, le temps joue contre vous : un virus sur un poste informatique peut se propager via un réseau local et paralyser tout le système d'information de l'entreprise. Un site de vente en ligne inaccessible se solde par une baisse du chiffre d'affaire et une image de l'entreprise dégradée auprès des clients et partenaires.

Cette notice explique la démarche suivre en cas d'attaque informatique.

But(s) d'une attaque informatique

Un pirate informatique poursuit principalement deux objectifs : faire commerce de données récupérées illégalement et, moins fréquemment, manifester un mécontentement - politique le plus souvent – que l'on appelle « *hacktivisme* » (contraction de *hacker*[2] et activisme).

[1] Documents téléchargeables sur le site du CLUSIF : http://bit.ly/RU67ml
[2] Hacker : mot anglais pour désigner un pirate informatique.

Les attaques opportunistes

Une attaque opportuniste ne cible pas une entité en particulier. Leur but est d'attaquer le plus grand nombre de systèmes d'Information dans l'espoir d'en toucher plusieurs. Les auteurs d'attaques opportunistes agissent souvent par le biais d'e-mailing contenant un lien vers un site Internet malicieux[3] ou une pièce jointe infectée par un programme malveillant.

Ces attaques peuvent être directes lorsque leur victime et leur cible sont une même entité. Dans le cas d'un *phishing*, le pirate manipule l'internaute afin d'obtenir des informations confidentielles (des coordonnées bancaires, par exemple).

Les attaques opportunistes indirectes, ou lancées par robots, sont aussi très répandues et souvent méconnues des entreprises. Il s'agit de prendre le contrôle d'un ordinateur pour relayer une attaque visant une cible bien déterminée. Cette technique permet ainsi aux hackers de brouiller les pistes d'éventuels enquêteurs.

Un pare-feu[4] bien configuré, un logiciel anti-virus à jour et une vigilance accrue des courriels entrants permettent d'éliminer la majorité des attaques opportunistes.

Remarque :

Les pirates informatiques se servent de plusieurs ordinateurs dont ils ont pris le contrôle pour lancer des attaques ciblées. Ce réseau de machine est appelé *botnet*.

Les attaques ciblées

Ce sont potentiellement les plus dangereuses, car le pirate informatique prépare son attaque en exploitant une faille de sécurité qu'il a identifiée chez sa cible. Les attaques ciblées visent donc une entité en particulier.

L'espionnage industriel est une des principales motivations des pirates informatiques fomentant ces attaques. Les entreprises ayant par exemple développé des procédés innovants, travaillant dans certains secteurs d'activité même en tant que sous-traitant (domaine militaire, aéronautique, pharmaceutique,…) ou encore répondant à un appel d'offre important doivent donc être particulièrement vigilantes.

[3] Site malicieux : sites hébergés sur un serveur sous contrôle de l'attaquant.
[4] Pare-feu : Firewall en anglais.

Attaques les plus courantes

Infection du système d'information

- **Comprendre l'attaque**

Selon la dernière enquête du CLUSIF, « Menaces Informatiques et Pratiques de Sécurité en France - Edition 2012 »[5], les infections par virus restent encore la première cause d'incident d'origine malveillante dans les entreprises françaises.

Les sites web malicieux, les pièces jointes infectées (email) et les supports amovibles (clés USB publicitaires, par exemple) sont les principaux vecteurs de virus ou de vers[6].
Les logiciels antivirus à jour, doivent détecter dans les 3 à 5 jours maximum la présence de ces fichiers ou logiciels malveillants sur un ordinateur.

Une activité anormale, la présence de fichiers corrompus ou le ralentissement du système peuvent être autant de signes d'infection d'un ordinateur. Première règle, **il faut agir vite** pour éviter qu'elle ne se propage sur tout le disque dur voire aux autres ordinateurs connectés au réseau.
Il faut donc d'abord déconnecter l'ordinateur d'Internet et l'isoler du réseau local sans pour autant débrancher la prise électrique car des données importantes pourraient être perdues.

- **Comment réagir ?**

  - *Désinfection*

La désinfection n'est pas toujours possible dans l'immédiat. Il faut laisser le temps aux concepteurs de logiciels antivirus de mettre à jour leur produit.
Un « Live CD » ou « Live USB » devra ensuite être téléchargé sur Internet. Ces programmes antivirus démarrent directement à partir du lecteur CD (ou USB) sans utiliser le système d'exploitation (Windows, OS X). L'ordinateur est scanné et désinfecté.
Il en existe de nombreux sur Internet, il faut néanmoins télécharger un nouveau fichier à chaque nouvelle infection pour s'assurer d'avoir la version la plus récente de la base de données virale.

Attention !

Une désinfection par un antivirus peut éventuellement effacer des fichiers systèmes infectés. L'ordinateur désinfecté risque donc de ne plus démarrer. Il ne faut pas hésiter à vous faire accompagner par un professionnel.

  - *Restauration du système et des données*

En cas d'infection sérieuse, il est conseillé de formater le disque dur et de procéder à une réinstallation complète pour repartir sur des bases saines, sans oublier de mettre à jour toutes les applications utilisées.

Il est préférable de restaurer les données sauvegardées au préalable. Si les données n'ont pas été sauvegardées régulièrement, il convient de les faire analyser par un antivirus à jour avant de les réintégrer sur l'ordinateur désinfecté.

[5] Cette enquête est téléchargeable sur le site du CLUSIF : http://bit.ly/MOnPCz
[6] Ver : logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, puis de l'exécuter sur ces mêmes cibles. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.

- **Se prémunir d'une nouvelle attaque**

Il est impératif que le logiciel antivirus soit à jour, de même que l'ensemble des applications installées sur le poste (navigateur Internet ou lecteur de PDF par exemple).

Intrusion dans le système d'information

- *Comprendre l'attaque*

Les intrusions dans le système d'information sont en principes évitées grâce à la mis en place d'un pare-feu. Elles consistent à ouvrir une porte sur le système d'information pour en prendre tout ou partie le contrôle.
Les signes d'une intrusion s'avèrent moins facile à détecter qu'une infection. On peut néanmoins s'inquiéter si des fichiers suspects ont été créés ou ont disparu, si des comptes ont été créés ou détruits, si le système montre une activité inhabituelle (très importante, à des horaires improbables).

- **Comment réagir ?**

- *Isoler l'ordinateur*

Il faut tout d'abord déconnecter l'ordinateur d'Internet et du réseau local de l'entreprise. Il ne doit toutefois pas être éteint car, pour comprendre comment le pirate est entré dans le système d'information, il est nécessaire d'identifier les processus actifs au moment de l'intrusion.

- *Trouver des traces*

Traiter une intrusion s'apparente à un jeu de piste pour trouver par quelle « porte » le pirate est entré. Cette démarche est du ressort de spécialistes en informatique (administrateurs systèmes ou réseaux, responsable infrastructure).

En premier lieu, il convient de réaliser une « copie physique » du disque dur, c'est-à-dire une image à un instant T du système. Une simple sauvegarde des fichiers ne fournit pas l'intégralité des informations contenues sur le disque dur, comme les secteurs non occupés.
Des applications disponibles sur Internet permettent de réaliser cette « copie physique ».

Il faut ensuite rechercher des modifications dans le système, les fichiers de configuration et les données de l'entreprise. Des outils et des données peuvent aussi avoir été installés par l'intrus. Enfin, l'activité sur le système doit être examinée de près.

- *Restaurer le système*

La seule manière de s'assurer qu'un ordinateur ne possède plus de porte dérobée ou autre modification opérée par l'intrus est de ré-installer complètement le système d'exploitation et d'appliquer tous les correctifs de sécurité avant de reconnecter la machine au réseau de l'entreprise.

Il est également conseillé de modifier les mots de passe car l'intrus a pu installer un « renifleur de mot de passe » aussi appelé « *sniffer* » ou « *keylogger* ».

- **Se prémunir d'une nouvelle attaque**

➢ Vérifier que la porte dérobée ne pourra plus être ouverte
➢ Configurer son pare-feu

Phishing

- **Comprendre l'attaque**

Le p*hishing* est une forme d'escroquerie en ligne[7]. On parle d'hameçonnage en français. Par extension, un phisher désigne l'émetteur du phishing.

Les phishers de masse usurpent l'identité d'un organisme connu (une banque, Visa, Paypal, Ebay) ou un service de messagerie électronique (Hotmail, Yahoo!, Gmail,…) en envoyant un courriel avec le logo de cette entité.

Dans le corps du message, le destinataire est invité à fournir des informations personnelles sous un faux prétexte. Très souvent cette demande revêt un caractère urgent et suscite l'envie (promesse d'une somme d'argent), ou la peur chez le destinataire (dépenses, conséquences désagréables).

Ces emails frauduleux contiennent généralement un lien renvoyant vers un site Internet imitant celui de l'organisation dont l'identité a été usurpée (site malicieux). L'interface, la charte graphique, la typographie, les noms et l'enchaînement des pages sont identiques.

Même l'URL vise à tromper l'internaute : https://www.lc1.fr (le second L est le chiffre 1), par exemple. C'est sur ces sites fantômes que la victime est invitée à saisir des informations confidentielles : mot de passe (de messagerie, de compte sur un site marchand), coordonnées bancaires…
Les données saisies par l'internaute sont envoyées au pirate informatique. Leur utilisation est ensuite très rapide avant que la supercherie ne soit découverte : achats sur Internet, création de faux papiers, récupération d'informations intéressantes sur les messageries, etc.

Les antispams (à jour) et pare-feu doivent filtrer ce type d'email frauduleux. Néanmoins, certains passent au travers des mailles du filet et réussissent tous les jours à manipuler des internautes.

- **Comment réagir ?**

Il faut immédiatement prévenir l'organisation dont l'identité a été usurpée afin d'être couvert en cas de retrait d'argent. L'email d'hameçonnage doit être conservé comme preuve.
Modifier immédiatement les mots de passe communiqués au site malicieux.

[7] Ce terme résulte de la contraction des mots anglais phreaking (activité de détournement téléphonique) et fishing (pêche).

Enfin, la tentative de phishing peut être signalée sur le site www.internet-signalement.gouv.fr. Il est également possible de porter plainte en cas de préjudice.

- **Se prémunir d'une nouvelle attaque**

Le meilleur moyen de se protéger du phishing reste encore la connaissance – et la mise en pratique - de quelques règles de sécurité qu'il ne faut pas hésiter à diffuser largement dans l'entreprise.

- **Etre critique vis-à-vis de l'email reçu** : est-il normal que je reçoive un message de cet émetteur ? Le contenu du message est-il conforme à ce que je peux attendre de cet émetteur (orthographe, grammaire, formulations malvenues) ?

- **Ne jamais divulguer d'informations confidentielles ou personnelles** en réponse à un email, même si celui-ci semble provenir d'une organisation reconnue.

- **Ne pas saisir directement** des informations personnelles dans des formulaires reçus par email

- **Se méfier** d'un email émis par un inconnu, invitant à une action urgente

- Si l'email émane d'un organisme reconnu, **regarder s'il ne comprend pas un nombre anormal de fautes de frappe ou d'orthographe**

- **Vérifier que la page web est sécurisée** au moment de saisir des données confidentielles. Pour cela, vérifier :
  - que l'URL de la page commence par https
  - qu'un cadenas fermé est présent en haut ou en bas de la page
  - qu'en cliquant sur ce cadenas on peut afficher le certificat en cours de validité assurant que la page est cryptée

Défacement ou défiguration de site Internet

- **Comprendre l'attaque**

Le terme « défacement » provient de l'anglais *defacing*. Un défacement de site consiste à défigurer la page d'accueil d'un site. Il s'agit en général d'hacktivistes souhaitant faire passer un message politique en affichant des images choquant l'opinion. Parfois, le hacker veut juste s'amuser ou montrer ses compétences de hacker.

Les sites défacés peuvent être unis (page blanche) ou porter la mention « hacked » (piraté) ou encore contenir toute sorte d'images selon le but du hacker.

- **Comment réagir ?**

Il faut tout d'abord trouver la faille de sécurité exploitée par le pirate en commençant par vérifier que le CMS[8] intègre les dernières mises à jour de sécurité de l'éditeur. Demander ensuite à un spécialiste de vérifier les « logs » (tableau de bord de suivi de l'activité sur site), afin de repérer toute activité anormale et de déterminer la manière dont le pirate a procédé.

Les identifiants et mots de passe d'accès au CMS devront être modifiés. Puis, la restauration de la sauvegarde du site permettra de lui redonner son aspect originel.

Il faut enfin vérifier qu'aucun fichier système n'a été modifié par le pirate.

- **Se prémunir d'une nouvelle attaque**

Les sites développés en interne - à partir de CMS open source notamment - doivent impérativement intégrer les mises à jour de sécurité publiées régulièrement sur Internet.
Les sites développés par un prestataire sont normalement protégés contre le défacement. En cas d'attaque, c'est à lui de rechercher les raisons d'une sécurité défaillante.

Attaque en déni de services

- **Comprendre l'attaque**

Une attaque en déni de service ou DoS (Denial of Service attack) consiste à bloquer le serveur hébergeant une messagerie ou un site Internet dans le but de les rendre indisponibles. Pour ce faire les pirates exploitent des failles de sécurité ou submergent le serveur de requêtes.

[8] CMS : Content Management System (système de gestion de contenu), logiciel permettant de concevoir et mettre à jour un site Internet.

Ces attaques peuvent avoir des objectifs divers : chantage, censure, démonstration de force, représailles,…

- **Comment réagir ?**

Il faut d'abord prévenir son opérateur pour qu'il active un système de nettoyage filtrant directement les flux d'attaque à détruire.

Il est déconseillé de céder aux chantages. Au contraire, les victimes d'attaques en déni de service doivent porter plainte.

- **Se prémunir d'une nouvelle attaque**

Il est difficile et coûteux de se protéger de ce genre d'attaque. Il faut demander à son hébergeur d'ajouter un autre serveur, uniquement dédié à l'analyse du trafic sur le site. Les attaques sont supprimées et le trafic normal est redirigé sur le serveur du site.

Porter plainte

Selon l'enquête biennale du CLUSIF « Menaces Informatiques et Pratiques de Sécurité en France », en 2012, 6% des entreprises ont déposé plainte suite à des incidents liés au SI[9].

Pourtant, la loi Godfrain[10] relative à la fraude informatique datant de 1988 stipule que « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de* ***2 ans d'emprisonnement et de 30 000 euros d'amende****.*

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de ***3 ans de prison et de 45 000 euros d'amende****.* »

[9] Document téléchargeable sur le site du CLUSIF : http://bit.ly/MOnPCz

Qui contacter ?

Avant de porter plainte, il faut réunir :

- Toute trace des dégâts engendrés par l'attaque (logs, traces d'un cheval de Troie,…) voire une copie physique du disque dur sur un support de sauvegarde magnétique

- L'adresse postale exacte des machines attaquées : adresse de l'entreprise s'il s'agit d'un ordinateur ou celle de l'hébergeur du serveur du site Internet

- La liste des préjudices subis : vol, suppression de données, blocage d'un site ayant entrainé une perte de chiffre d'affaires,…

- **La BEFTI**

La Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) est un service de la Police Judiciaire[11] dévolu aux infractions informatiques sur la région parisienne :

- Intrusion dans un ordinateur ou un réseau
- Contrefaçon de logiciels ou de bases de données
- Téléchargements illégaux
- Piratage de réseau téléphonique
- Défacement de sites sensibles
- Modification ou suppression de données
- Défaut de sécurisation des données personnelles
- Collectes frauduleuses, illicites ou déloyales de données à caractère personnel

[10] Loi Godfrain : Loi n° 88-19 du 5 janvier 1988
[11] Site de la BEFTI : http://bit.ly/gvyzPA

La BEFTI enregistre les plaintes, participe à la recherche des pirates et analyse les supports récupérés lors des perquisitions.

BEFTI :
122/126, rue du Château des Rentiers
75013 Paris
Tél. : 01 55 75 26 19
pppj-befti-information@interieur.gouv.fr

- **L'OCLCTIC**

L'Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication[12] (OCLCTIC) a les mêmes missions que la BEFTI mais sur tout le territoire français.
Des policiers (investigateurs en cybercriminalité) et des gendarmes (N-Tech) sont répartis dans toute la France.

Les coordonnées de l'enquêteur spécialisé le plus proche sont fournies par les commissariats et les gendarmeries.

- **LA DCRI**

Dans le cadre de ses missions, la Direction Centrale du Renseignement Intérieur a pour vocation d'accompagner les entreprises victimes d'attaques informatiques.
Les coordonnées des délégations régionales peuvent être obtenues auprès des commissariats.

RESPONSABILITES DES ENTREPRISES

Plus qu'une nécessité, protéger ses données devient une obligation légale. Les défaillances de sécurité qui rendaient hier l'entreprise victime en cas d'intrusion ou de blocage de site, peuvent désormais la rendre responsable pénalement, voire coupable.

En effet, l'article 34 de la loi Informatique et Libertés stipule que le responsable du traitement des données à caractère personnel[13] dans l'entreprise « *est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».
En cas de manquements graves à ces obligations, le « responsable du traitement » (le chef d'entreprise) risque jusqu'à 5 ans de prison et 300 000€ d'amende.

[12] Site de OCLCTIC : http://bit.ly/UIN0OY
[13] Données à caractère personnel : toute information relative à une personne physique identifiée ou qui peut être identifiée : cordonnées, adresse email d'un client, d'un salarié…