

LUTTER CONTRE LA CYBERCRIMINALITÉ



SOMMAIRE



Introduction	page 4
Rappel des risques et des pratiques	pages 5 à 8
Quelques règles de base	pages 9 à 15
Et si malgré tout	page 16
Sites utiles	page 17
Glossaire	pages 19 à 23



INTRODUCTION

Alors que le numérique fait partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages.

Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de l'image de l'entreprise.

Les experts s'accordent à dire que le **maître mot est la sensibilisation**.

Ce guide nous permet de faire le point sur les dangers et les solutions techniques possibles, mais aussi les "bonnes pratiques" pour s'en prémunir.

**IDÉE REÇUE :
LES MULTINATIONALES SONT LES PRINCIPALES VICTIMES DES CYBER
PIRATES !!**

La plupart des **petites entreprises et des associations**, mais également les **personnes individuelles**, ne sont pas convaincues que les cybercriminels s'intéressent à elles. Elles pensent à tort être éloignées de ce problème ou être à l'abri. Pourtant, les cybercriminels seront sans doute plus tentés de s'en prendre à elles du fait de l'absence de conscience du risque et de moyens financiers, matériels et humains pour apporter des réponses adéquates au regard de la sécurité.

ETAT DES LIEUX : QUELQUES CHIFFRES :

Au cours des deux dernières années, les cyberattaques représentent les menaces les plus courantes pour l'entreprise.

En France, 77% d'entre-elles visent les PME et les organismes de moins de 250 employés. Alors que la cybercriminalité a doublé au cours de cette période, 50% déclarent ne disposer d'aucun plan de réaction.



RAPPEL DES RISQUES ET DES PRATIQUES - ÉNONCÉ DES CYBERMENACES ET DES VULNÉRABILITÉS

De nombreux pirates utilisent les réseaux sociaux pour monter des fraudes à l'entreprise. Un risque que les dirigeants et les salariés doivent prendre en compte dans leurs pratiques de ces outils. À en croire le Ministère de l'Intérieur, les escroqueries de type « fraude au président » ou « fraude au changement de RIB » auraient fait perdre aux entreprises françaises pas moins de 485 millions d'euros entre 2010 et 2015.

Cyber attaques typiques : ce sont bien des cyberattaques !

LES CAS LES PLUS FREQUENTS :

- **Rançongiciels** : ou ransomware = virus d'extorsion : envoi d'un virus malveillant qui va chiffrer et endommager voire rendre inutilisable le système informatique : + 113 % en 2015 dans le Monde !

Vecteurs : Lien «spam» ou fichier infecté : **avec paiement de la rançon** (400 à 4000 €) **dans les délais pour disposer de la clé de décryptage et espérer retrouver les informations initiales. Demande pressante payable en "Bitcoins"**

Exemple :

Un DAF se connecte sur son informatique et constate que toute la comptabilité de l'entreprise a disparu...quelqu'un a dû cliquer sur un lien piégé ou sur une pièce jointe infectée et un "cheval de Troie" s'est introduit, rendant le système inutilisable...il reçoit, peu de temps plus tard un e-mail lui demandant une rançon, associée à une minuterie qui décompte le temps restant...

- Le hameçonnage

Il désigne les différentes techniques utilisées pour soustraire des informations sensibles. Le principe consiste non pas à utiliser une faille informatique mais une "faille humaine" en dupant les internautes par le biais d'un **courriel (phishing)**, d'un **appel (vishing)** ou d'un **sms (smishing)** apparemment sûr. Il emprunte le plus souvent l'identité d'une entreprise de confiance et demande à l'internaute de mettre à jour des informations le concernant via un formulaire factice. Les pirates réussissent à obtenir identifiants, mots de passe ou encore données personnelles ou bancaires (numéros de client ou numéro de compte en banque). Conséquence : les hackers peuvent transférer directement de l'argent sur un autre compte.

• Faux ordres de virement (FOVI) : escroquerie

L'**escroquerie** est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 € d'amende. (Code Pénal-Art.312-1 et 313-1).

Pour mettre en place ces fraudes aux ordres de virement (FOVI), les escrocs recueillent des informations (réseaux sociaux, Google, presse spécialisée, registre du commerce, société.com...) sur les entreprises ciblées.

Des données précieuses qui leur permettront non seulement d'usurper, de manière crédible, l'identité d'un dirigeant de l'entreprise ou d'un de ses fournisseurs, mais aussi d'identifier la personne (assistante de direction, comptable...) avec qui entrer en contact (téléphone, courriel, réseaux sociaux...) pour lancer l'arnaque.

Les **attaques** sont **préparées**, et se font lors de **conditions favorables** (déplacement du dirigeant à l'étranger).

Exemple :

Un individu se faisant passer pour le dirigeant (avec usurpation du n° d'appelant et modification de la voix, aujourd'hui techniquement possible), demandant à une assistante de faire un virement "urgent et confidentiel". Mise en œuvre de techniques d'intimidation, de flatterie ("vous étiez très en beauté lors de la cérémonie à Paris avec votre robe rouge" (l'assistante portait effectivement une robe rouge photo publiée sur FB), de menace aussi si la personne ne s'exécute pas.

• Vols de données personnelles et bancaires sensibles à l'insu de l'entreprise :

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende (Code Pénal – Art 323-3).

Ces données deviennent "**monnayables**" sur le "**Darknet**" où existent offres et demandes réelles.

Darknet : Les DarkNets sont distincts des autres réseaux car le partage y est anonyme (c'est-à-dire que les adresses IP ne sont pas partagées publiquement).

Exemple :

Le Cheval de Troie : "je rentre, je prends, je disparaiss..."

Un hacker crée un site de logiciels très connus, gratuits (ex : retouche de photos, antivirus gratuit), dans lesquels il va introduire des logiciels malveillants...pendant l'installation du logiciel, le cyberpirate va accéder à toutes les données en moins de 5 minutes (code secret, données bancaires) et pourra ainsi aller puiser dans le compte, en toute liberté.

LES PRINCIPALES ETAPES :

- Ciblage de la victime.
- Courriel argumenté usurpé avec invitation à ouvrir un fichier pourvu d'un code malveillant.
- Courriers postaux classiques ou fax
- Ingénierie sociale par flatterie ou pression - usurpation du numéro de téléphone et de l'adresse de messagerie.
- Utilisation des réseaux sociaux pour récolter des informations (sur l'entreprise, les dirigeants, les salariés).
- Contact avec la banque : courriel et/ou n° de téléphone usurpés pour procéder au virement à l'étranger.
- Répartition rapide des montants et blanchiment.
- Exfiltration des données : contrôle des flux – cryptage.
- Effacement des traces.



LES PRINCIPALES TECHNIQUES DE FRAUDE

Phishing

un email provenant – soi-disant - d'un organisme officiel vous demande de cliquer sur un lien, qui renvoie vers un site pirate chargé de récupérer vos données de connexion Banque en Ligne ou de CB



Vishing



un appel vous demande de valider une opération bancaire en communiquant vos données confidentielles, ou d'appeler un serveur vocal pour effectuer cette vérification



Smishing

un sms ou mms vous invite à appeler un serveur vocal interactif ou à cliquer sur un lien frauduleux, pour y saisir vos données bancaires



Un seul objectif : subtiliser vos données bancaires sensibles en vous incitant à les saisir dans un formulaire web ou à les communiquer par téléphone ou sms

Les appâts les plus utilisés



Pour vous protéger au mieux d'une cyber attaque, voici quelques règles de base à appliquer



Choisir avec soin ses mots de passe, en suivant notamment les conseils de l'ANSSI

Ce procédé, seul, ne suffit pas à protéger vos informations mais il n'en demeure pas moins indispensable. Il convient de choisir des mots de passe difficiles à retrouver à l'aide d'outils automatisés ou par une tierce personne. Il doit être difficile à trouver mais facile à retenir ! Pour vous aider, il existe aussi des logiciels gestionnaires de mots de passe.

Choisissez des mots de passe d'au moins 10 ou 12 caractères composés de lettres majuscules et minuscules, de chiffres et de caractères spéciaux, n'ayant aucune référence personnelle (nom, date de naissance, prénom des enfants....). Les logiciels de décryptage ne prennent pas forcément en compte toutes ces variables. Les mots figurant dans le dictionnaire sont à proscrire car il existe aussi des « attaques par dictionnaire » qui consistent à tester à grande vitesse, via un logiciel spécialisé, tous les mots du dictionnaire en espérant que l'un d'eux soit utilisé comme mot de passe. Les codes d'accès du type « maison » ou « chocolat » ne tromperont pas les hackers.

Pour le mémoriser plus facilement, vous pouvez utiliser :

- La méthode phonétique : « j'ai acheté 8 CD pour 100 euros cet après-midi » devient : ght&CD%€7am (attention : exemple connu, à ne pas utiliser tel quel).

- La méthode des premières lettres (parole de chanson, proverbe ou autre) : «j'ai un pantalon noir et blanc qui me va très bien » devient : g1pN&Bqmvbtb

- La répétition d'un mot de passe : choisir un mot de passe de 5/6 caractères et le doubler

- N'utilisez pas le même mot de passe pour tous vos comptes. Les mots de passe protégeant des contenus sensibles (banque,...) ne doivent pas être réutilisés pour d'autres services. Il peut suffire de ne changer qu'un seul caractère.

- Changez-les régulièrement (tous les 3 mois est un bon rythme).

- Ne divulguez à personne vos mots de passe.

- Ne les conservez pas dans un fichier ou sur un post-it !

- N'utilisez pas la retenue automatique des mots de passe.

- Verrouillez votre poste de travail lorsque vous vous absentez, même brièvement.

- Préconisez l'utilisation d'un coffre-fort numérique de type "keepass".



Mettre à jour régulièrement ses logiciels

Des vulnérabilités existant dans chaque système d'exploitation, les éditeurs proposent régulièrement aux utilisateurs des mises à jour de sécurité.

- Veillez à ce que votre ordinateur dispose d'un pare-feu et d'un logiciel antivirus, et activez les mises à jour automatiques du système (windows ou Mac).

- Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement quand c'est possible sinon téléchargez les correctifs de sécurité disponibles en veillant à n'utiliser pour cela que les sites internet officiels des éditeurs.



Effectuer des sauvegardes régulières

En procédant à des sauvegardes régulières de vos données, vous éviterez de vous exposer à une perte trop importante de fichiers si vous avez été piégés.

- Effectuez des sauvegardes régulières (hebdomadaires par exemple), en privilégiant un hébergement sécurisé chez un prestataire agréé par l'ANSSI. Si vous choisissez un périphérique externe, ne le laissez pas branché à votre ordinateur car le « ransomware » peut également crypter les dossiers qui se trouvent à l'intérieur. Stockez-le de préférence dans un autre lieu de façon à ce qu'il ne soit pas détruit comme vos données d'origine en cas d'incident (inondation, incendie, vol...). Une attention particulière doit être apportée à la durée de vie de ces supports.



Etre vigilant avec l'utilisation du Wi-Fi

Un Wi-Fi mal sécurisé permet plus facilement à des personnes d'utiliser votre connexion dans le but de réaliser des opérations malintentionnées. D'autre part, faites preuve vous-même d'une grande vigilance lorsque vous utilisez un Wi-Fi public.

- Préférez une installation filaire au Wi-Fi.
- Ne divulguez votre clé de connexion qu'à des personnes de confiance et pensez à la changer régulièrement.
- Evitez d'utiliser les WI-FI publics (réseaux disponibles dans les aéroports,...) ou seulement pour une navigation web générale.
- Préférez un réseau Wi-Fi privé et sécurisé ou la 3G ou 4G de votre téléphone.
- Pensez à désactiver votre appareil après chaque connexion.



Appliquer les mêmes règles de sécurité à tous ses appareils

L'emploi de téléphones connectés (ordiphones, smartphones), d'ordinateurs portables et de tablettes facilite et accélère le transport et l'échange de données. Des risques et des menaces supplémentaires pèsent sur la sécurité des informations que vous emportez ou que vous échangez.

- N'installez que les applications de source fiable et nécessaires à leur utilisation.
- Bannissez les applications intrusives.
- Installez un code de verrouillage sur l'écran d'accueil et activez la fonction verrouillage automatique.
- Ne préenregistrez pas votre mot de passe (voir consigne n°1).
- Soyez vigilant avec les équipements qui vous sont offerts. Ils peuvent contenir des logiciels malveillants. Les clés USB, de par leurs multiples vulnérabilités, sont un vecteur d'infection privilégié par les attaquants.
- Ne rechargez pas vos équipements sur les bornes électriques libre-service. Certaines peuvent avoir été conçues pour copier les documents à votre insu.
- Ne connectez pas vos équipements à des postes ou des périphériques informatiques qui ne sont pas de confiance.



Faire attention au phishing !

Simple et accessible, l'email est une arme de choix pour les cyberattaques. La technique de « l'hameçonnage » ou « phishing » consiste à envoyer un mail d'apparence inoffensif qui redirigera la victime vers une pièce jointe contenant un virus ou vers un faux site où elle devra rentrer des coordonnées personnelles.

- Assurez-vous de l'identité de l'expéditeur du mail et en cas de doute ne pas hésiter à le contacter directement.
- Détruisez les messages que vous aurez identifiés sans hésitation comme frauduleux, dans lesquels on remarque beaucoup de fautes d'orthographe, de tournures de phrases étranges ou des histoires invraisemblables.
- Méfiez-vous du mail se faisant passer pour un tiers de confiance (administration,...) et qui vous demande de mettre à jour vos informations personnelles. Si vous cliquez, vous êtes alors renvoyé sur un site qui, à première vue, apparaît comme authentique mais qui est pourtant bien factice. Sachez que, de manière générale, les banques, les centres d'impôts ou les organismes sociaux ne demandent jamais de transmettre des données personnelles sensibles ou pièces justificatives par mail. Ne répondez évidemment pas à ce mail mais si vous pouvez prenez tout de même le temps de le signaler à l'entreprise qui est imitée ainsi que sur le site du gouvernement prévu à cet effet.
- Méfiez-vous également d'un mail que vous pourriez croire venir de l'une de vos connaissances qui vous demande une aide rapide (un virement la plupart du temps). Cela peut signifier que votre connaissance a été victime d'une attaque et que le hacker tente « d'hameçonner » ses contacts.
- Ne jamais ouvrir une pièce jointe ou suivre un lien dont l'expéditeur est soit inconnu, soit d'une confiance relative car un simple clic sur une image ou un lien suffit pour installer à votre insu un logiciel ou code malveillant (cheval de Troie) sur votre ordinateur.
- N'ouvrez pas et ne relayez pas de messages de type chaînes de lettres, appels à la solidarité, alertes virales...
- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse anti-virus avant de les ouvrir.



Savoir utiliser l'internet avec précaution

Les achats sur internet réclament une grande prudence. Via smartphones et tablettes, ils sont de plus en plus communs, mais il est important de se méfier lors de son shopping. En effet, ces terminaux font face à de nombreuses menaces et sont souvent moins bien sécurisés que les ordinateurs. Mais dans tous les cas :

- Effectuez vos transactions uniquement sur des sites sécurisés. Vous les reconnaitrez à leur adresse internet commençant par « *https* » et non par « *http* », le « s » en plus signifiant que la connexion est sécurisée. Contrôlez la présence d'un cadenas dans la barre d'adresses.
- Privilégiez lors du règlement en ligne de votre commande la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS ou par tout autre moyen d'authentification forte proposé par votre banque. Utilisez des mots de passe distincts et robustes pour vos activités sensibles (banque, sites administratifs,...).
- N'hésitez pas à vous rapprocher de votre banque pour connaître et utiliser les moyens de paiement sécurisés qu'elle propose. Le service e-carte bleue par exemple vous permet de régler vos achats à distance (Internet, téléphone) sans avoir à transmettre les coordonnées de votre carte bancaire. A chaque achat, vous ne transmettez qu'un e-numéro à usage unique délivré en temps réel.
- Utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur internet : une adresse réservée aux activités importantes (banque, sites administratifs,...) et une adresse destinée aux autres services en ligne (forum, jeux concours,...).
- Assurez-vous de fermer votre session après avoir visité un site qui demande d'entrer de l'information personnelle sensible.
- Videz la mémoire cache de votre navigateur pour ne laisser aucune trace de vos transactions.
- Eteignez votre ordinateur après usage.



En entreprise, sensibiliser ses collaborateurs !

En matière de cyberattaque, une bonne protection de l'entreprise passe par la sensibilisation des collaborateurs. Chacun d'eux représente un maillon de la chaîne qui peut permettre, à son insu, de nuire à l'organisation.

- Etablissez des règles basiques en matière de Cybersécurité au sein de votre organisation et incitez vos collaborateurs à les respecter.
- Dissociez l'usage personnel de l'usage professionnel de vos appareils connectés.
- Incitez vos collaborateurs à la plus grande prudence sur les réseaux sociaux (ne pas divulguer d'information même minime de type professionnel).

Une récente étude permet de faire le point sur les pratiques des professionnels en matière de gestion des médias sociaux. Il en ressort que seuls 40 % des sondés affirment avoir paramétré leurs comptes sur les réseaux sociaux (LinkedIn, Facebook...) pour réserver à leurs seuls contacts l'accès aux données de leur profil. L'étude montre également que la majorité des sondés accepte d'interagir avec des inconnus sans avoir pris le soin de vérifier leur identité.



Contrôler avec soin la communication externe de l'entreprise

- Pour décourager les escrocs, la première chose à faire est de tarir la mine de données sur laquelle ils s'appuient pour bâtir la fraude. Les informations sensibles relatives à l'entreprise doivent sinon disparaître d'Internet, du moins être en accès sécurisé. Il s'agit notamment des organigrammes grâce auxquels les pirates vont reconstruire la chaîne de validation des ordres de paiement, mais aussi des coordonnées à l'aide desquelles les contacts directs seront pris. Ces recommandations doivent être suivies par tous les acteurs de l'entreprise (salariés, dirigeants) notamment dans l'usage qu'ils font, à titre privé comme professionnel, des médias sociaux. Les enjeux sont importants. De nombreuses entreprises ont tout simplement disparu après avoir subi une fraude aux ordres de virement.



ET SI MALGRÉ TOUT...

Vous n'avez pas eu le temps de mettre en œuvre les conseils et préconisations de ce guide, ou bien les attaquants ont réussi à les contourner...ne cédez pas à la panique et adoptez les bons réflexes...

- Déconnecter le poste d'internet et du réseau de l'entreprise pour stopper l'attaque.
- Alerter (par téléphone ou de vive voix) son entourage professionnel (l'envoi de courriels, est, à ce moment, fortement déconseillé).
- Si un FOVI a été émis, prévenir sa/ses banques le plus rapidement possible pour optimiser les chances de bloquer le(s) virement(s) avant qu'il ne soit trop tard.
- En cas de doute sur l'intégrité d'un poste ou du réseau informatique, faire un balayage scan de l'ordinateur au moyen d'un logiciel antivirus à jour pour vérifier s'il est infecté, et, le cas échéant, éliminer le virus.
- Procéder à une restauration complète avec des sauvegardes saines et récentes (sauvegarde quotidienne hébergée hors site à préconiser)
- Faire appel à un expert prestataire informatique si le fonctionnement de l'ordinateur est toujours compromis.
- Faire rechercher les traces disponibles liées à l'attaque (un équipement n'étant jamais isolé dans un système d'information, des traces de compromission doivent exister dans d'autres équipements).
- Après l'incident, réinstaller complètement le système d'exploitation à partir d'une version saine, supprimer tous les services inutiles, restaurer les données d'après une copie de sauvegarde non compromise.
- Changer tous les mots de passe du système.
- Procéder au dépôt de plainte (commissariat ou gendarmerie) conserver des « captures d'écran » afin de donner des éléments de preuve aux enquêteurs.
- Lister tous les préjudices subis.



SITES UTILES :

- Site de pré-plainte en ligne du Ministère de l'Intérieur: <https://www.pre-plainte-en-ligne.gouv.fr>
- Portail officiel de signalement des contenus illicites du web (Ministère de l'Intérieur): <https://www.internet-signalement.gouv.fr>
- Campagne d'information du CIGREF : la «Hack Academy» <https://www.hack-academy.fr/>
- Site de l'ANSSI : Agence nationale de la Sécurité des Systèmes d'Information: <http://www.ssi.gouv.fr>
- Ordres de virement : 9 réflexes «sécurité»: <http://www.fbf.fr/fr/files/9T9GRN/Guide-securite-1.pdf>
- Les conseils CNIL pour un mot de passe efficace: <https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe>
- Site officiel de la plateforme de lutte contre les spams vocaux et SMS sur télécoms offrant le dispositif de signalement en ligne et toute l'information: <http://www.33700.fr/>

Restez vigilant !



Ne donnez pas suite à un email, sms ou numéro de téléphone d'une personne inconnue



Ne cliquez pas sur un lien dans un email, sms ou mms non attendu



Relisez bien chaque email, sms ou mms reçu. Les fautes d'orthographe ou de grammaire sont un indice



vérifiez que votre connexion est sécurisée pour vos paiements en ligne



Protégez votre ordinateur, tablette et mobile avec un logiciel anti-virus et anti-malware



Ne téléchargez rien depuis un email, sms ou mms non attendu

Aucune banque ou organisme public ne vous demandera par email, sms, mms ou appel des renseignements personnels et confidentiels

GLOSSAIRE



Cybercriminalité : "Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible."

Attaque informatique : Terme générique désignant une action malveillante dont la cible ou le moyen est l'informatique.

Canular ("Hoax") : Information vraie ou fausse, souvent transmise par messagerie électronique ou dans un forum, et incitant les destinataires à effectuer des opérations ou à prendre des initiatives, souvent dommageables.

Remarque :

Il peut s'agir d'une fausse alerte aux virus, de chaîne de solidarité, pétitions, promesse de cadeaux, etc. Quelques canulars fréquents sont répertoriés sur des sites dédiés comme « Hoaxbuster » ou « Hoaxkiller ».

Capteur clavier, enregistreur de frappes ("Keylogger", "keystroke logger") : Logiciel ou matériel employé par un utilisateur malveillant pour capturer ce qu'une personne frappe au clavier.

Remarque :

Cette technique permet de voler efficacement les mots de passe, les données bancaires, les messages électroniques, etc.

Bombardement de courriels ("Mail Bombing") : Forme de déni de service contre les systèmes de messageries par l'envoi en grand nombre de courriels à un destinataire ciblé, dans une intention malveillante.

Chantage ("Ransomware") : Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Si ce dernier refuse de payer ou d'effectuer une tâche imposée, le service auquel il veut accéder lui est refusé par le code malveillant.

Cheval de Troie ("Trojan Horse") : Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante. Le code malveillant dissimulé permet de prendre le contrôle de l'ordinateur compromis à l'insu de l'utilisateur légitime. Un virus comporte généralement un cheval de Troie.

Remarque :

La fonction cachée exploite parfois les autorisations légitimes d'une entité du système qui invoque ce programme. Elle peut par exemple permettre la collecte frauduleuse, la falsification ou la destruction de données.

Chiffrement : Transformation cryptographique de données produisant un cryptogramme.

Cyberdéfense : Ensemble des mesures permettant à un État de défendre dans le cyberspace les systèmes d'information jugés essentiels.

Cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La Cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une Cyberdéfense.

Code malveillant ("Malware", "Malicious software") : Programme développé dans le but de nuire au travers d'un système informatique ou d'un réseau; chevaux de Troie, virus et vers sont des codes malveillants.

Cyberattaque : Acte malveillant envers une cible informatique, généralement via un réseau de télécommunications.

Cybermenace : Action menaçante locale ou à distance visant l'information ou le système d'information.

Déni de service ("Denial of Service", "DoS") : Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.

Espiogiciel ("spyware") : Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.

Filoutage ou hameçonnage ("phishing") : Technique trompeuse visant à obtenir des renseignements personnels en abusant les détenteurs. Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

Remarque :

Les sites sont reproduits, après avoir été aspirés. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique.

Ingénierie sociale ("Social Engineering") :

Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes.

Remarque :

Il s'agit, pour les personnes malveillantes usant de ces méthodes, d'exploiter le facteur humain, qui peut être considéré dans certains cas comme un maillon faible de la sécurité du système d'information.

IP ("Internet Protocol") : Protocole de communication fondé sur des adresses numériques distinguant les machines connectées, segmentant la communication en paquets, et comportant une adresse IP source et IP adresse de destination lors d'une session.

Machine piratée ou "zombie" : Machine compromise incluse dans un réseau ("botnet") contrôlé par un contrôleur de ce réseau de "zombies".

Pare-feu ("Firewall") : Un pare-feu (ou garde-barrière) est un outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

Pirate informatique ("Hacker") : Individu s'introduisant dans un système informatique souvent par défi intellectuel, pas toujours par intention malveillante, ou par profit.

Porte dérobée ("Backdoor") : Accès logiciel ou matériel permettant à un individu de se connecter à une machine distante de façon furtive.

Remarque :

Une porte dérobée peut également être la cause d'une mise en œuvre incorrecte d'un protocole.

Pourriel, pollurriel ("spam") : Tout courrier électronique non sollicité par le destinataire.

Remarque :

Le courrier est souvent envoyé simultanément à un très grand nombre d'adresses électroniques. Les produits les plus vantés sont les services pornographiques, la spéculation boursière, des médicaments, le crédit financier, etc.

Réseau de robots ("botnet") : Réseau de machines compromises conçu pour permettre la transmission des ordres à tout ou partie de ces machines et diriger une attaque déguisée en masse sur une seule ou sur plusieurs cibles déterminées par un système de commande et contrôle (C2) administré.

Usurpation d'adresse ("Address Spoofing") : Action malveillante qui consiste à utiliser délibérément l'adresse d'un autre système en lieu et place de la sienne.

Remarque :

Il faut rapprocher cette action de l'usurpation d'identité, considérée comme un délit par le droit pénal français. L'idée est de faire passer son système d'information pour un autre. L'adresse usurpée peut être une adresse MAC (pour Medium Access Control), une adresse IP, une adresse de messagerie.

Ver ("Worm") : Un ver (ou worm) est un 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.

Remarque :

Les deux termes ver et virus sont relativement proches. Un ver est un virus qui se propage de manière quasi autonome (sans intervention humaine directe) via le réseau. Les vers sont donc une sous-catégorie de virus, dont le vecteur primaire de propagation reste le réseau.

Virus : Un virus est un programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et, bien souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Le mode de survie peut prendre plusieurs formes: réplication, implantation au sein de programmes légitimes, persistance en mémoire, etc. Pour sa propagation, un virus utilise tous les moyens disponibles: messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB...



cress
Chambre Régionale
de l'Économie Sociale
et Solidaire Occitanie

BANQUE POPULAIRE
DU SUD
ADDITIONNER LES FORCES
MULTIPLIER LES CHANCES



Conception et impression

