LA SECURITE INFORMATIQUE

MATTHIEU IZAC BTS SIO1

[Tapez le résumé du document ici. Il s'agit généralement d'une courte synthèse du document. Tapez le résumé du document ici. Il s'agit généralement d'une courte synthèse du document.]

SOMMAIRE

Quelques définitions :

◆ La cyber sécurité

La cyber sécurité comprend tous les moyens permettant d'assurer la protection et l'intégrité des données (sensibles ou non) au sein d'une infrastructure numérique. C'est une majeure dans le métier des systèmes d'information. Le concept de cyber sécurité est revenu à plusieurs reprises en raison de la transformation numérique des entreprises, qui utilisent des outils informatiques et communiquent sur Internet en général.

En gros, la cyber sécurité assure une gestion des données dans des conditions optimales et sûres. Il permet la protection des systèmes d'information et des données diffusées contre les personnes dites cybercriminelles. Les compétences informatiques acquises par un attaquant constituent un risque à ne pas prendre à la légère. De l'installation d'un logiciel antivirus à la configuration des serveurs en passant par la sécurisation des centres de données et des bureaux, la sécurité informatique touche tous les secteurs.

◆ La cyber criminalité

La cyber criminalité désigne enfaite toute activé dites illégale perpétrée a l'aide d'ordinateurs ou d'internet. Les criminels ou les pirates son des individus, aussi bien que des groupes organisés ou encore des cellules financées par le gouvernement qui ont pour buts d'exécuter des cyber attaques à travers de diverses techniques comme par exemple le phishing (voir définition page 3), l'ingénierie sociale ou tout autre type de malware.

La cyber criminalité est un sujet d'autant plus d'actualité de nos jours avec la professionnalisation et la prolifération de celle-ci qui entrainent chaque année d'innombrables dommages extrêmement couteux, qui impactent les individus des entreprises et mes les gouvernements. D'après des études les dommages provoqués par la cybercriminalité s'élèvent a 6 billions de dollars par en an en 2021 ce qui en fait l'une des activités criminelles si ce n'est pour dire la plus lucrative qui soient.

Quelques définitions :

◆ Le phishing

Le phishing ou encore hameçonnage est une forme d'escroquerie sur internet. Elle a pour but de voler vos informations personnelles comme le numéro de compte, codes personnels etc. Pour ce faire un fraudeur se fait passer pour un organisme que l'on a connaissance comme une banque, un service d'impôt ou encore la CAF en utilisant le même logo et le même nom d'organisme ou en créant une réplique exacte du site de ces organismes la dans l'optique de crée une façade pour que vous rentrez vos informations en pensant que vous êtes sur le vrai site. Cette arnaque se fait généralement via un mail ou un message vous invitant à « confirmer » ou « mettre à jour vos informations suite à un incident technique »

◆ Le malware

Un malware, ou logiciels malveillants sont définitions comme leurs noms l'indiquent par leurs intentions malveillantes, ce sont des logiciels qui agissent contre les exigences de l'utilisateur de l'ordinateur. Ils sont utilisées par les pirates ou le gouvernement pour voler des renseignements. Ils peuvent notamment chiffrer ou supprimer des données ou encore espionner un utilisateur.

On peut citer plusieurs malware comme le :

- Le cheval de Troie : c'est un malware qui agit comme à l'époque grecque avec le fameux cheval de Troie. Les attaques de chevaux de Troie ont recours à la tromperie dans le but de duper des utilisateurs afin qu'ils exécutent des programmes bénins en apparence mais qui cachent en réalité leur jeu malveillant.
- Le ransomware : c'est un type de programme malveillant qui a pour but de chiffrés et volés des fichiers d'utilisateur afin de forcer ceux-ci a payer une rançon pour que leurs fichiers soit divulguer

Qu'est ce que la CNIL ?

La Commission Nationale de l'Informatique et des Libertés (CNIL) a été créée par la loi Informatique et Libertés du 6 janvier 1978. Elle est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. Ainsi, elle est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. La CNIL est une autorité administrative indépendante (AAI), c'est-à-dire un organisme public qui agit au nom de l'Etat, sans être placé sous l'autorité du gouvernement ou d'un ministre. Elle est composée de 18 membres élus ou nommés et s'appuie sur des services. Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction.

Qu'est ce que l'ANSSI ?

L'anssi est un acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.