République Algérienne Démocratique Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université d'Ibn Khaldoun – Tiaret

Faculté des Mathématiques et de l'Informatique

Département Informatique

Thème

[Ingénierie sociale et les attaques réseaux]

Pour l'obtention du diplôme de Master

Spécialité : Réseaux & Télécom

Rédigé par : Hassas mohamed amine

Hor tayeb

Dirigé par : Bekkar khaled

Année universitaire 2013-2014

Dédicace

<< A nos parents >>

<<A nos profs>>

<< A nos familles>>

<< A nos amis >

Hassas Mohamed Amine

Dédicace

<< A nos parents >>

<<A nos profs>>

<< A nos familles>>

<< A nos amis >

Hor Tayeb

Remerciements

On dit souvent que le trajet est aussi important que la destination. Les cinq années de maîtrise nous ont permis de bien comprendre la signification de cette phrase toute simple. Ce parcours, en effet, ne s'est pas réalisé sans défis et sans soulever de nombreuses questions pour lesquelles les réponses nécessitent de longues heures de travail.

Nous tenons à la fin de ce travail à remercier « ALLAH » le tout puissant de nous avoir donné la foi et de nous avoir permis d'en arriver là.

En premier lieu nous tenons à remercier Monsieur Bekkar Khaled, notre encadreur, qui nous a fait découvrir le monde passionnant de la recherche et avec qui nous avons eu le plaisir de mener tous nos travaux de mémoire. Son entière disponibilité et ses merveilleuses explications ont été précieuses.

Nous souhaitons également faire part de nos reconnaissances à tous les enseignants qui nous ont éclairés la voie du savoir durant notre cycle.

Un grand merci également à l'ensemble du personnel pédagogique, technique et administratif du département, principalement mes condisciples lors de la formation.

Nous tenons à exprimer notre profonde gratitude à toutes celles et ceux qui nous ont apporté leur soutien, leur amitié ou leur expérience tout au long de ce travail de mémoire.

Résumé

L'ingénierie sociale ("social engineering") est une technique qui vise à accéder à des informations confidentielles ou à certains actifs par la manipulation de personnes qui y ont accès directement ou indirectement. Le « phishing » (hameçonage) est un exemple d'ingénierie sociale.

L'ingénierie sociale ne s'applique pas seulement au domaine de l'informatique, elle peut survenir dans la vie de tous les jours et plus particulièrement sur le lieu de travail. A partir du moment où des actifs ayant un certain intérêt sont en jeu, des attaques de ce type peuvent apparaître.

Le facteur humain est le point central des techniques d'attaque rencontrées dans l'ingénierie sociale. En essence il s'agit de la manipulation intelligente de notre propension naturelle à faire confiance. Des relations de confiance ne reposant sur rien de concret sont mises en place de manière calculée, mais le plus souvent par simple discussion, et exploitées par la suite pour tirer un maximum de profit de la situation.

L'ingénierie sociale peut se faire via téléphone, courrier électronique, via des réseaux sociaux et bien sûr en présence physique de l'attaquant

Mot-clé : ingénierie, sociale, attaque, réseau, sécurité, informatique

Sommaire

Introduction Générale

Le développement des nouvelles technologies de l'information et de la communication ont grandement modifié les pratiques en matière de sécurité. Lorsque l'on parle de protection de l'information, les solutions technologiques se sont avérées un choix logique et efficace. Par contre, cette tendance à appliquer une solution technologique a eu pour effet pervers de négliger le facteur humain. Peu importe à quel point un système de sécurité est sophistiqué et complexe, il y aura toujours un être humain pour contrôler ce système. Dans son environnement de travail, de tous les jours, l'humain doit faire des choix et prendre des décisions qui peuvent avoir des conséquences importantes pour la sécurité de l'entreprise. Si l'humain est l'élément central de toute organisation, il représente également l'élément le plus vulnérable, car il est à la fois la cause de nombreux incidents et la partie maîtresse dans la protection de l'information. Faisant partie à la fois de la solution et du problème, il est essentiel de s'attarder à son comportement et de comprendre pourquoi il est vulnérable. En fait, il est surprenant de constater à quel point l'élément humain est vulnérable et facilement exploitable.[3]

L'ingénierie sociale, qui est l'art d'utiliser la tromperie et le mensonge pour arriver à ses fins (Mitnick, 2006), exploite précisément ce maillon faible de la chaîne de sécurité.[3]

En parlent pour le 1er chapitre sur la sécurité des réseaux et informatiques, ensuite sur l'ingénierie sociale pour le 2eme chapitre.

En fin nous donnons la mise en pratique de l'ingénierie sociale et des conseilles pour la sécurité des informations et des réseaux.

Chapitre1 : Sécurité informatique et réseaux

Introduction

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques.

I- Services de sécurité

L'ISO a défini six services de sécurité : authentification, contrôle d'accès, confidentialité et intégrité des données, non-répudiation et protection contre l'analyse du trafic. Différents types de mécanismes (chiffrement, signature numérique, listes de contrôle d'accès, bourrage, notarisation…) servent pour assurer ces services. Ils diffèrent par leur sophistication, leurs coûts, les efforts nécessaires pour leur implantation, leur maintenance et leurs besoins en ressources humaines. [4] [5]

1- Authentification

Le service d'authentification garantit l'identité des correspondants ou des partenaires qui communiquent. On distingue deux cas d'authentification simple et un cas d'authentification mutuelle :

- L'authentification de l'entité distante. Elle garantit que le récepteur est celui souhaité. Son action peut intervenir à l'établissement de la communication ou pendant le transfert des données. Son objectif principal est la lutte contre le déguisement, également appelé usurpation d'identité (spoofing).

- L'authentification de l'origine. Elle assure que l'émetteur est celui prétendu. Le service est inopérant contre la duplication d'entité. Comme le précédent, il s'agit d'authentification simple.

- L'authentification mutuelle. Elle assure que les deux entités émettrice et réceptrice se contrôlent l'une l'autre.

Le service d'authentification est inutilisable dans le cas d'un réseau fonctionnant en mode sans connexion : dans les réseaux, comme dans la vie courante, l'authentification nécessite un échange entre les deux partenaires.

Exemple: À la banque, pour prouver votre identité, vous montrez une carte nationale d'identité. Le guichetier effectue un rapide contrôle visuel, entre votre visage et la photo qui est sur la carte. Il y a bien échange entre vous et le guichetier. Un niveau de sécurité supplémentaire consiste à vous faire signer en présence du guichetier : celui-ci vérifie la signature manuscrite présente sur la carte. Dans les deux cas de cet exemple, le guichetier fait confiance aux autorités qui délivrent la carte d'identité pour avoir vérifié l'authenticité de votre identité. Si vous avez volé la carte d'identité, saurez-vous aussi ressembler à la photo et imiter la signature en temps réel ?

2- Contrôle d'accès

Le service de contrôle d'accès empêche l'utilisation non autorisée de ressources accessibles par le réseau. Par « utilisation », on entend les modes lecture, écriture, création ou suppression. Les ressources sont les systèmes d'exploitation, les fichiers, les bases de données, les applications… Pour contrôler les accès aux ressources, il faut d'abord authentifier les utilisateurs afin de s'assurer de leur identité qui est transportée dans les messages d'initialisation et ensuite établir une liste des droits d'accès associés à chacun. L'annuaire LDAP fournit en général les données nécessaires à la mise en œuvre d'un tel mécanisme.

3- Confidentialité des données

Garantir la confidentialité des données empêche une entité tierce (non autorisée, le plus souvent en état de fraude passive) de récupérer ces données et de les exploiter. Seuls les utilisateurs autorisés doivent être en mesure de prendre connaissance du contenu des données. Un message ou un échange de messages a sa confidentialité garantie dès lors que tout utilisateur

non autorisé qui aurait pu le récupérer ne peut pas l'exploiter. Il n'est pas obligatoire de mettre en place des procédures pour empêcher cette « récupération ».

Exemple : Certaines chaînes de télévision payantes sont transmises cryptées de telle sorte que seuls les possesseurs de décodeurs appropriés peuvent regarder leurs émissions favorites. Les autres peuvent toujours rester devant un écran zébré !

4- Intégrité des données

Garantir l'intégrité des données assure au récepteur que les données reçues sont celles qui ont été émises. Les données ont pu être altérées, de manière accidentelle ou de manière délibérée à la suite d'une fraude active. On distingue différents niveaux de service selon les mécanismes mis en œuvre. Peut-on détecter que des données ont été modifiées ? Si oui, peut-on récupérer les données initiales ? Sait-on détecter les données supplémentaires, insérées à tort ou délibérément ? Peut-on détecter les données manquantes et les récupérer ? Peut-on détecter que des données a priori correctes ne sont que des doublons de données déjà reçues ?

Par ailleurs, l'intégrité possède une portée plus ou moins grande (le message complet ou un champ spécifique du message seulement). Lorsque la communication a lieu en mode non connecté, seule la détection des modifications peut être mise en œuvre. Les principes de la protection contre les erreurs : ajouter un bloc de contrôle d'erreur qui est le résultat d'un algorithme connu appliqué au message. Le récepteur refait le calcul sur le message qu'il a reçu et compare les deux blocs de contrôle d'erreurs. Il vérifie ainsi l'intégrité du message, cette seule méthode est insuffisante pour détecter des messages insérés dans un flux de données. Les protections mises en œuvre s'inspirent du même principe.

5- Non-répudiation

La non-répudiation de l'origine fournit au récepteur une preuve empêchant l'émetteur de contester l'envoi d'un message ou le contenu d'un message effectivement reçu. La non-répudiation de la remise fournit à l'émetteur une preuve empêchant le récepteur de contester la réception d'un message ou le contenu d'un message effectivement émis.

Exemple : Vous postez un courrier en « recommandé avec accusé de réception ». La Poste ajoute à votre courrier un document qui sera signé par le récepteur et qui sera ensuite renvoyé à l'expéditeur. Pour vous, la possession de cet accusé de réception interdit au récepteur de prétendre qu'il n'a rien reçu. La Poste joue un rôle d'intermédiaire entre vous et votre correspondant, elle rend le service de non-répudiation du courrier… Dans cette opération, elle ne vérifie pas votre identité et encore moins le contenu de votre lettre ! Votre correspondent peut soutenir avoir reçu une envelope vide.

6- Protection contre l'analyse de trafic

Le secret du flux lui-même empêche l'observation du flux de transmission de données, source de renseignements pour les pirates. Ce cas s'applique aux situations où on a besoin de garder la confidentialité sur l'existence même de la relation entre les correspondants.

II- Domaines d'application de la sécurité informatique

Pour une organisation, toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité d'un système d'information.[1]
En fonction de son domaine d'application la sécurité informatique se décline en (figure 1) :

- sécurité physique et environnementale ;
- sécurité de l'exploitation ;
- sécurité logique, sécurité applicative et sécurité de l'information ;
- sécurité des infrastructures informatique et de télécommunication (sécurité des réseaux, sécurité Internet et cybersécurité).

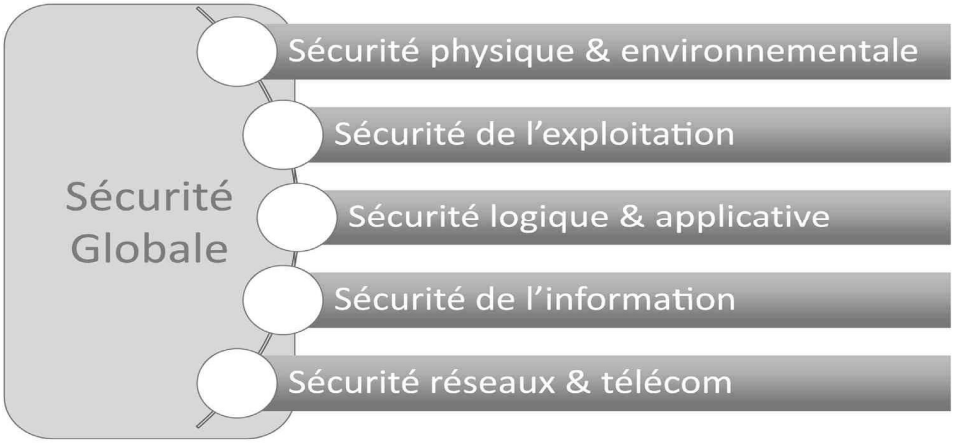

Figure 1 : Domaines d'application de la sécurité.

1- Sécurité physique et environnementale

La sécurité physique et environnementale concerne tous les aspects liés à la maîtrise des systèmes et de l'environnement dans lesquels ils se situent.

2- Sécurité de l'exploitation

La sécurité de l'exploitation doit permettre un bon fonctionnement opérationnel des systèmes informatiques. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jour.

La sécurité de l'exploitation dépend fortement de son degré d'industrialisation, qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches. Bien que relevant de la responsabilité de l'exploitation, ces conditions concernent très directement la conception et la réalisation des applications elles-mêmes et leur intégration dans un système d'information.

3- Sécurité logique, applicative et sécurité de l'information

La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes, des services offerts et à la protection des données.

La sécurité applicative comprend le développement pertinent de solutions logicielles (ingénierie du logiciel, qualité du logiciel) ainsi que leur intégration et exécution harmonieuses dans des environnements opérationnels.

4- Sécurité des télécommunications

La sécurité des télécommunications consiste à offrir à l'utilisateur final et aux applications communicantes, une connectivité fiable de « bout en bout ». Cela passe par la réalisation d'une infrastructure réseau sécurisée au niveau des accès au réseau et du transport de l'information (sécurité de la gestion des noms et des adresses, sécurité du routage, sécurité des transmissions à proprement parler) et cela s'appuie sur des mesures architecturales adaptées, l'usage de plates-formes matérielles et logicielles sécurisées et une gestion de réseau de qualité.

La sécurité des télécommunications ne peut à elle seule garantir la sécurité des informations. Elle ne constitue qu'un maillon de la chaîne sécuritaire car il est également impératif de sécuriser l'infrastructure informatique dans laquelle s'exécutent les programmes. Pris au sens large, cela comprend la sécurité physique et environnementale des systèmes (poste de travail de l'utilisateur, serveur ou système d'information.

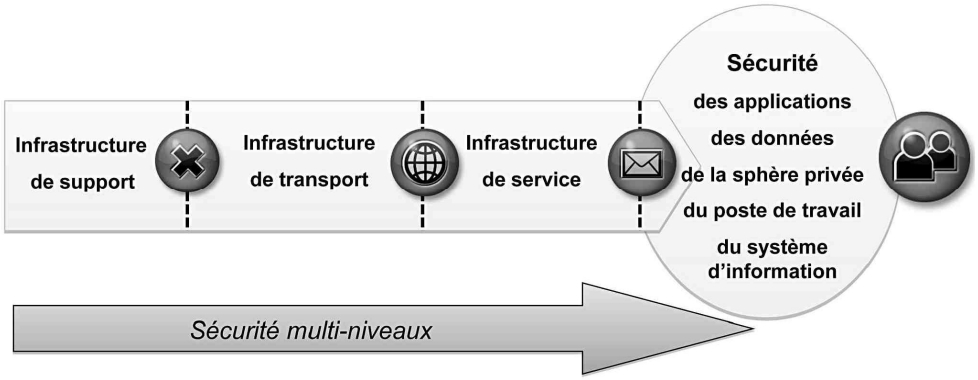

Figure 2 : Sécurité des infrastructures de télécommunication.

5- Facettes de la sécurité

- Maîtrise de la sécurité informatique, procédures qui régissent leurs utilisations et configuration.
- La sécurité repose sur des axes complémentaires managériaux, techniques et juridiques qui doivent être abordés en parallèle. Elle n'est jamais acquise définitivement.
- Veille juridique.
- Actions d'information et de formation, mesures préventives et dissuasives.[2]

III- Techniques d'attaques

Le piratage informatique est en constante évolution et l'éventail des techniques est aujourd'hui très large. Voici quatre techniques de base, régulièrement utilisées par les hackers.[6]

1- Le social engineering

L'ingénierie sociale, ou social engineering en anglais, n'est pas à proprement parler une technique d'attaque. Il s'agit plutôt d'une méthode de persuasion permettant d'obtenir des informations auprès de personnes exerçant des postes clés. Aucune compétence technique n'est nécessaire. Le principe n'est pas de cibler des failles techniques, mais des failles humaines. L'imposture, le mensonge, la duperie sont les principaux leviers de l'ingénierie sociale. Un exemple : téléphoner à l'administrateur réseau, en se faisant pour une entreprise de sécurité, afin d'obtenir des informations précieuses sur le système mis en place. Tous le succès de l'opération réside dans le talent de persuasion du hacker. Kevin Mitnick, le plus célèbre des hackers, a réalisé plusieurs de ses exploits en exploitant simplement la crédulité d'employés des sociétés ciblées.

2- Le défaçage

Cette technique a pour but de modifier un site web en y insérant du contenu non consenti par son propriétaire. Le défaçage est utilisé principalement par des hackers militants qui souhaitent ainsi dénoncer les pratiques de certains gouvernements ou entreprises. Pour

« défacer » le site, le hacker exploite le plus souvent une faille de sécurité du serveur web qui l'héberge. Elle peut par exemple être décelée au niveau du système d'exploitation du serveur. Ce type d'attaque est en général revendiquée, l'objectif étant de donner un maximum d'audience à ce détournement afin de décrédibiliser la cible. Parmi les récents défaçages, citons celui du site de Marine Le Pen, hacké en avril dernier. La page d'accueil affichait pendant quelques heures une photo d'une jeune femme coiffée d'un foulard accompagnée d'un message en arabe disant : « Le site a été hacké en réponse à la considération que vous avez pour la femme musulmane en France ». Après un retour à la normale, le site est une nouvelle fois défacé quelques heures après. La page d'accueil affichait cette fois avec une image promotionnelle des jeux « Mon Petit Poney ». En cliquant sur l'image, l'internaute était renvoyé vers la page « racisme » de Wikipedia.

3- Le déni de service distribué (DDoS)

Une attaque par déni de service distribué vise à saturer un service afin de le rendre inaccessible. Les cibles typiques de ce type d'attaque sont les serveurs web. Une fois saturés, ils vont rendre indisponible le ou les sites internet qu'ils hébergent. Initialement, le déni de service (DoS) était réalisé par un hacker isolé depuis une seule machine. Mais la technique a rapidement évoluée vers une attaque réalisée à partir d'un maximum de machines, d'ou l'appellation « distribué ». Ces machines « zombies » auront été préalablement infectées par du code malveillant transmis par exemple sous la forme d'un e-mail piégé. L'infection est le plus souvent effectuée en toute discrétion, sans effets visible sur le système. L'objectif du hacker est d'y installer, en toute discrétion, les outils nécessaires au lancement de la future attaque. Une fois son armée de machines zombies constituée, le hacker peut lancer une attaque simultanée depuis l'ensemble des ordinateurs corrompus. En face, le serveur va « tomber » sous le nombre de requêtes.

4- Le Buffer Overflow

Le principe d'une attaque par Buffer Overflow ou « dépassement de mémoire tampon », est de provoquer une défaillance dans un programme afin de le pousser à attaquer les protections d'un système. Un « buffer » est une zone de mémoire temporaire utilisée par un programme. Le dépassement de mémoire survient lorsque cet espace reçoit plus de données qu'il ne peut

normalement en contenir. Résultat : le programme va bugger. Le hacker exploite alors ce bug pour faire exécuter du code malveillant au programme défaillant. Ce code aura par exemple pour mission de modifier la politique de sécurité du système et ainsi d'ouvrir des accès normalement protégés. Un des programmes typiquement ciblé par ce type d'attaque est le navigateur internet. La défaillance est provoquée en ouvrant un e-mail compromis ou en naviguant sur un site web piégé.

IV- La criminalité informatique

Les ordinateurs font partie intégrante de la vie des citoyens et des entreprises. Internet est devenu l'un des moyens les plus importants d'information et de communication.[2][1]

La loi décrit quatre nouveaux délits relatifs à la criminalité informatique :

- le faux en informatique
- la fraude informatique
- la manipulation de données
- le « Hacking »

1- Faux en informatique

Constituer un faux en informatique consiste à modifier ou à effacer des données d'un système informatique ou à modifier l'utilisation de ces données, de manière à entraîner également la modification de leur portée juridique.

Cette notion a été introduite pour mettre fin aux problèmes que suscitait la notion de « faux en écriture » appliquée aux données informatiques. En effet : les données contenues dans un ordinateur sont-elles, oui ou non, considérées comme des écrits ?

2- Fraude informatique

La fraude informatique est la variante informatique de l'escroquerie au sens classique du terme. L'escroquerie consiste à soutirer, au moyen de belles paroles et de propositions, des biens ou des fonds à des personnes qui ne se doutent de rien. Quand quelqu'un utilise à cette fin des moyens de communication modernes, le législateur considère qu'il s'agit également

d'escroquerie. Internet permet, dans un délai rapide et à moindres frais, de toucher un grand nombre de victimes.

3- La manipulation de données

3-1- Transactions financières

Il vous est peut-être arrivé de recevoir un e-mail vous proposant de grosses sommes d'argent à changer ou à blanchir. L'arnaque consiste à vous faire croire qu'il est possible d'encaisser d'importants bénéfices excédentaires d'une instance soi-disant officielle. Cet e-mail sollicite votre aide : on vous demande de verser de l'argent ou transmettre des documents d'entreprise. En échange, on vous promet une participation aux bénéfices de l'ordre de 20 % ou plus.

Il existe, dans cette catégorie, un autre type de criminalité : le « phishing ». Par ce procédé, des criminels reproduisent des sites d'entreprises ou d'organisations connues pour voler des données personnelles, des mots de passe et des sommes d'argent.

3-2- Loteries ou jeux de hasard

Vous recevez par e-mail un avis vous indiquant que vous avez gagné le gros lot à une loterie ou à un jeu de hasard. Pour recevoir votre prix, vous devez d'abord verser une somme d'argent.

Les loteries officielles ne fonctionnent pas de cette manière : vous ne pouvez recevoir un prix qu'après avoir acheté un billet de loterie, un billet à gratter ou un bulletin de loto. La loterie ne prend jamais contact avec le gagnant : ce dernier doit en prendre l'initiative.

Parier n'est pas punissable. En revanche, exploiter des jeux de hasard sans une autorisation de la Commission des jeux de hasard l'est effectivement. Selon la loi sur les jeux de hasard, il est interdit en Belgique d'exploiter des jeux de hasard ou des établissements de jeux de hasard, sous quelque forme, dans quelque lieu et de quelque manière que ce soit. Seul un nombre d'établissements défini par le législateur peuvent organiser des jeux de hasard. Cela signifie donc que les casinos et les jeux d'argent en ligne sont toujours illégaux en Belgique.

3-3- Héritages

Vous recevez par courriel un avis d'un soi-disant organe officiel étranger ou d'un soi-disant « notaire » étranger. Ce message précise qu'après de longues recherches, on a pu vous identifier comme étant le (seul) héritier d'une personne très riche récemment décédée. Mais attention : pour pouvoir recueillir l'héritage, vous devez d'abord verser une somme d'argent, destinée soi-disant à régler tous les frais administratifs. Vous comprenez dès lors qu'il ne s'agit pas ici d'un vrai notaire, mais bien d'escrocs qui en veulent à votre argent.

3-4- Investissements exotiques

Vous recevez par e-mail des propositions (malveillantes) d'investissements dans des projets exotiques, avec promesses de gains astronomiques à la clé. Bien entendu, il s'agit ici encore de fraude.

3-5- Passeports, visas, documents, ...

Les escrocs tentent aussi de jouer sur vos sentiments. Dans certains e-mails par exemple, on vous demande de verser de l'argent pour quelqu'un qui a besoin de toute urgence d'un passeport, d'un visa ou d'un autre document officiel. Pour vous apitoyer, l'e-mail décrit avec force détails les conditions de vie déplorables d'un pays situé à l'autre bout du monde. L'argent que vous devriez verser servirait à payer l'intermédiaire chargé de délivrer le document. Il va de soi que vous ne verrez jamais cette personne et que vous aurez tout simplement perdu votre argent …

3-6- Achats sur Internet

On peut acheter à peu près tout sur Internet. Mais tous les vendeurs ne sont pas fiables. Certains, surtout à l'étranger, ne livrent pas les biens achetés et payés.

3-7- Ventes sur Internet

Vous placez une annonce sur Internet dans le but de vendre quelque chose. Une personne ou une entreprise accepte l'offre sans même discuter le prix demandé. L'escroc peut alors procéder de différentes manières : il vous donne un chèque sans provision, vous demande de verser une garantie sur un compte à l'étranger …

4- Hacking

Hacking est une notion très vague. Même les informaticiens ne tombent pas d'accord sur la signification exacte du mot. Hacking consiste à pénétrer illégalement dans un système informatique. Cette « effraction » implique généralement une intention frauduleuse. Mais établir involontairement une connexion et la maintenir volontairement est également considéré comme du piratage. Même pirater un système informatique qui n'est pas ou à peine sécurisé est punissable.

Dans l'évaluation de Hacking, la loi distingue les 'insiders' des 'outsiders'. Les insiders sont des personnes qui ont une autorisation d'accès, mais qui outrepassent cette autorisation. Ces personnes ne sont punissables que si leur piratage cache une intention de nuire ou une intention frauduleuse. Pour les 'outsiders', cette restriction n'existe pas : ils sont dans tous les cas passibles de sanctions, même s'ils s'introduisent dans un système avec « de bonnes intentions ».

Il est interdit de collecter ou d'offrir – contre rétribution ou non – des données permettant des violations informatiques. Cette interdiction vise surtout à juguler le commerce de codes d'accès et de 'Hacking tools'.

Les pirates informatiques utilisent parfois un grand nombre « d'ordinateurs zombies ». Il s'agit d'ordinateurs individuels ou de sociétés mal protégés et infectés par un « cheval de Troie ». Le cheval de Troie est un programme qui permet à un malfaiteur de prendre le contrôle d'un ordinateur relié à Internet et de l'utiliser. Votre ordinateur peut lui aussi être intégré dans un tel réseau. Le pirate a ainsi le contrôle total sur votre ordinateur et a accès à vos données.

Protégez votre ordinateur contre le piratage, car une fois que quelqu'un y a accès, tout est possible : le pirate peut non seulement fureter à sa guise mais également utiliser votre ordinateur à des fins illégales ou détruire vos fichiers.

Conclusions

Actuellement, le problème est de correctement définir les risques engendres par la criminalité informatique. Il faut pour cela avoir une vision globale du problème et connaitre globalement les techniques utilises par les nouveaux flibustiers. Il s'agira ensuite d'analyser correctement les vulnérabilités propres à chaque site, de définir le niveau de sécurité requis et enfin de mettre en place une politique de sécurité acceptable. Lors de cette étape il faut bien veiller à examiner le problème tant du côté de l'administrateur que de celui du simple utilisateur afin de ne pas en créer de nouveaux. .[6]

Chapitre 2 : Ingénierie sociale

Introduction

L'ingénierie sociale est une technique de manipulation utilisant la tromperie, qui vise à obtenir l'accès à des informations confidentielles ou à des ressources à accès restreint par la manipulation de personnes en ayant directement ou indirectement l'accès. Cette analyse de l'ingénierie sociale est basée sur deux champs d'études distincts sans toutefois être nécessairement indépendants, soit la psychologie cognitive et la sociologie. Alors que la psychologie cognitive nous permettra de mieux comprendre les erreurs dans le processus décisionnel d'un individu, la sociologie nous permettra de mieux saisir comment nos interactions sont organisées et pourquoi elles représentent une vulnérabilité. Ces deux perspectives permettront de comprendre pourquoi l'ingénierie sociale est une menace constante pour la sécurité d'une organisation et comment elle exploite le facteur humain.[7]

I. Recension des écrits

L'ingénierie sociale existait bien avant l'avènement de l'informatique et il est difficile d'avancer qu'elle est plus utilisée aujourd'hui qu'il y a vingt ans. Cependant, à l'ère de l'information, les systèmes de la sécurité s'organisent et dépendent énormément des technologies au point de mettre l'être humain à un second niveau. Mais tout système de sécurité a un point en commun, il dépend à un moment ou un autre de l'être humain. L'ingénierie sociale attaque précisément ce point vulnérable qu'est l'être humain.

Il n'existe pas de consensus sur la définition de l'ingénierie sociale. Pour ce présent travail, nous utiliserons la définition du Cyberworld Awareness and Security Enhancement Structure, une initiative européenne soutenue par l'État du Luxembourg qui définit l'ingénierie sociale comme :

« Une technique de manipulation par tromperie qui vise à obtenir l'accès à des informations confidentielles ou à des ressources à accès restreint par la manipulation de personnes en ayant directement ou indirectement l'accès. » [3]

Comme la définition l'illustre, le facteur humain est le point central des attaques visées en ingénierie sociale. Plus souvent qu'autrement, des relations de confiance ne reposant sur rien de concret sont mises en place de manière calculée, le plus souvent par simple discussion, et elles sont exploitées afin de retirer un maximum de profit de la situation.

Les techniques d'ingénierie sociale sont fréquemment utilisées dans plusieurs domaines, notamment dans celui de la vente (voir Cialdini, 1993), car elles ressemblent en plusieurs points à de la manipulation. Elles visent à influencer ou à manipuler une personne, dans le cas de la vente, il s'agirait d'un acheteur potentiel, afin de lui faire dire ou de lui faire poser une action qui n'est pas totalement volontaire. Si ces techniques de manipulation représentent un outil avantageux pour un vendeur, il est possible de croire que ces techniques peuvent également être utilisées comme arme d'intrusion et menacer la sécurité d'une organisation.

Bien qu'il soit difficile d'évaluer la prévalence de l'ingénierie sociale comme menace à la sécurité, plusieurs exemples populaires illustrent bien la crédibilité de la menace. À ce titre, Kevin Mitnick est l'un des pirates informatiques les plus célèbres, car celui ci a été le premier à figurer sur la liste des dix personnes les plus recherchées par le FBI à la fin des années 1980. Il a piraté les bases de données de clients de Pacific Bell, de Fujitsu, Motorola, Nokia, Sun Microsystems, en plus d'accéder illégalement à un ordinateur du Pentagone. Mitnick, maintenant conseiller en sécurité de l'information, utilisait principalement l'ingénierie sociale, notamment par téléphone ou en personne, afin d'obtenir l'accès nécessaire au système. Ainsi, il a démontré qu'il est beaucoup plus simple de manipuler les gens afin d'obtenir l'information désirée plutôt que pirater les barrières de sécurité informatique. Ses livres, The Art of Deception:

Controlling the Human Element of Security (2003) et The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers (2005), illustrent bien l'efficacité de l'ingénierie sociale ainsi que le potentiel qu'elle représente. Cependant, il importe ici de faire la différence entre les attaques qui sont possibles (réalisées) et celles qui sont

probables (imaginées). Cette distinction permettra de s'éloigner des récits qui tiennent davantage de l'anecdotique que de la réalité.[3]

II. Méthodologie

Cette méthodologie est la plus accessible et la plus pertinente afin de bien comprendre les mécanismes à l'œuvre dans l'ingénierie sociale. Car bien qu'il s'agisse d'un phénomène répandu, il fait l'objet de peu d'études empiriques. Pour l'instant, la compréhension de l'ingénierie sociale en termes de menace pour la sécurité d'une entreprise n'a pas fait l'objet de beaucoup d'attention scientifique. Par cette étude, nous visons davantage à apporter des nouveaux éléments à la compréhension de l'ingénierie sociale qu'à évaluer sa prévalence. La présente étude propose l'analyse de l'ingénierie sociale à travers des dimensions individuelles et sociales dans le contexte particulier de la sécurité.[3]

1. Prise de décision en sécurité

Avant de débuter l'analyse des principes à la base de l'ingénierie sociale, il faut comprendre le contexte particulier de la sécurité dans lequel les gens doivent prendre des décisions. Tout d'abord, la sécurité, tout comme l'insécurité, est un concept abstrait et subjectif intimement lié à une action dans un espace à un temps donné. Fortement associée au sentiment, la sécurité est liée davantage à la perception du risque qu'à un calcul objectif et réaliste. Par exemple, ce qui représente un risque pour vous à votre domicile de Montréal n'en est pas un pour un résident de Rimouski. Dans le même ordre d'idées, la perception de la menace terroriste n'est pas la même avant et après les attentats du 11 septembre 2001.

La nature abstraite et subjective de la sécurité complexifie la prise de décision. Ceux qui utilisent l'ingénierie sociale ont bien compris qu'une décision en sécurité résulte d'un calcul coûts bénéfices difficilement opérable mentalement (West, Ryan, Mayhorn, Hardee et Mendel, 2009).

Car si on voit généralement peu de bénéfices à prendre une décision sécuritaire, il faut admettre que les coûts sont tout aussi difficiles à évaluer. Tout d'abord, les coûts sont souvent

absents, car la menace est invisible. Une personne aimable qui tente de vous aider avec un problème informatique ne représente pas un risque.

West et ALS (2009) soulèvent que la sécurité fait face à un défi tout aussi important, celui de l'apprentissage. Un grand nombre des comportements sont appris soit par l'imitation ou par le renforcement positif et négatif. Or, en sécurité, le renforcement négatif, qui se matérialise habituellement par des conséquences négatives, n'est pas immédiat, car, tout dépendant de la situation, il n'y a pas de conséquence à prendre une décision risquée. Même que le renforcement est parfois totalement absent, car le problème peut ne pas être détecté ou s'il l'est, il sera difficile d'identifier la source. Ensuite, on remarque qu'il y a également un manque important de renforcement positif en matière de sécurité. Généralement, une décision sécuritaire engendre peu de félicitations et attire peu de reconnaissance par le milieu de travail.

En fait, il y a peu de bénéfices sinon pas du tout à prendre des décisions sécuritaires. Cette absence de renforcement positif et négatif rend l'apprentissage difficile. Bref, la prise de décision en sécurité est un calcul très abstrait qui revient plus à l'intuition qu'à la logique. Cette intuition est faillible et manipulable.

III.Facteurs cognitifs

L'ingénierie sociale est une technique efficace, car elle profite des erreurs du cerveau humain dans le traitement de l'information et parce que l'humain est influençable et manipulable. Il est intéressant de constater que ces deux phénomènes amènent l'humain à poser des actions de manière instinctive. Ces actions bien inoffensives dans le quotidien peuvent représenter un risque non négligeable pour une entreprise. Car en agissant systématiquement face à des situations données, l'être humain est prédicable et exploitable.[3]

1. Biais de raisonnement

Bien que la prise de décision comporte généralement son lot d'incertitude, notamment face aux risques potentiels d'une décision, la psychologie cognitive a démontré que même si on possède toute l'information nécessaire, on prend souvent des décisions erronées. L'utilisation de raccourcis mentaux, les heuristiques, lors du traitement de l'information est à l'origine de ses erreurs de jugement. Les heuristiques sont souvent utilisées, car elles sont hautement économiques en temps et en énergie. Par contre, elles mènent à des biais sévères et systématiques. Les heuristiques sont fortement basées sur l'impression qui survient automatiquement et indépendamment de toute évaluation objective de la situation.

2. Perception du risque et biais d'estimation

La plupart du temps, notre perception du risque n'est pas représentative de la réalité de ce risque. Les gens surestiment plusieurs risques mineurs alors qu'ils négligent d'autres risques majeurs. Par exemple, on exagère les risques spectaculaires, rares, populaires, immédiats, incertains, hors de notre contrôle, nouveaux et moralement dérangeants. Cette perception du risque est profondément inscrite dans notre raisonnement et il est le résultat de plusieurs milliers d'années d'évolution (Schneier, 2008).

Comme nous avons mentionné, la perception du risque agit sur le comportement et joue un rôle prépondérant sur le processus de décision de l'individu. Considérant que le risque est faible, un individu ne procédera pas au traitement de l'information de manière aussi rigoureuse que s'il considérait le risque élevé.

L'un des biais à l'origine de cette mauvaise perception du risque est celui de l'excès de confiance. Les gens ont une image très positive d'eux mêmes et ils surestiment leurs propres habilités et connaissances (Alicke et Govorun, 2005). Cette présomption par excès de confiance incite les individus à prendre de mauvaises décisions à partir d'une information inadéquate et de stratégies décisionnelles inefficaces (Sternberg, 2007 : 453). On ne sait pas très bien pourquoi on procède par excès de confiance dans nos estimations ; on peut simplement l'expliquer par le refus de penser le faux.

L'humain surestime aussi sa capacité à contrôler son environnement. Ce biais, nommé illusion du contrôle (Taylor et Brown, 1988), signifie que l'humain a tendance à croire qu'il peut contrôler son environnement ou du moins l'influencer, alors qu'une évaluation objective n'attribuerait pas un tel pouvoir sur le même événement.

Ensuite, il y a le biais de la détection du mensonge, c'est à dire que les gens surestiment presque toujours leur capacité à détecter le mensonge (Marett, Biros et Knode, 2004). Ce biais devient encore plus problématique lorsque l'on considère le biais de vérité. Dans le biais de vérité, les gens sous estiment la possibilité que quelqu'un mente (Martin, 2004). Notamment à cause de ces biais, l'humain est très vulnérable à la manipulation.

L'humain a également tendance à croire que les mauvaises choses telles que la mort, les désastres naturels, un crime, un accident n'arrivent qu'aux autres (Armor et Taylor, 2002 ; Levine, 2003). Ce raisonnement, le biais d'optimisme, peut aussi être transposé à une organisation qui ne prend pas au sérieux certains risques et se croit protégé de tout. Il s'agit d'une illusion d'invulnérabilité qui amène l'humain à se croire peu susceptible de subir des conséquences négatives.

3. Information confirmatoire

Les gens ont tendance à chercher et sélectionner les informations qui confirment l'hypothèse de départ au détriment des informations qui prouvent qu'elle est fausse. C'est-à-dire que l'humain a une préférence pour les éléments qui confirment les croyances passées. Il est sélectif dans le choix des informations si bien que les nouvelles informations seront jugées pertinentes et riches seulement si elles sont en accord avec les croyances passées. De l'autre côté, lorsqu'elles vont à l'encontre des croyances de la personne, elles seront considérées comme inintéressantes ou erronées. Ce biais réduit considérablement la qualité de la décision (Kray et Galinsky, 2003), car de nouvelles informations pertinentes seront ignorées. Ce biais de raisonnement, aussi connu sous le nom d'ancrage, peut devenir un outil d'influence important, car il est généralement facile de cibler les croyances d'une personne. Une fois la cible placée dans une situation où elle doit prendre une décision, le pirate lui donne toute sorte d'information qui confirme ses croyances et qui joue à son avantage.

IV. Bases de l'influence

Les heuristiques peuvent être considérées comme des défaillances dans le traitement de l'information. Dans les pages qui suivent, nous présenterons des techniques d'influence fréquemment utilisées dans l'ingénierie sociale. Ces dernières représentent des manières concrètes d'exploiter les heuristiques. C'est l'activation de normes sociales et l'utilisation malhonnête de celle-ci qui rend l'humain vulnérable à la manipulation. Voici quelques techniques qui peuvent être utilisées afin de manipuler des employés pour leur soutirer de l'information.

L'être humain aime aider les autres et il est un être social. Par conséquent, l'une des techniques les plus simples, mais des plus efficaces pour influencer les gens, est d'être gentil. Être aimable avec les gens, assure une plus grande coopération de la part de la victime. Afin d'influencer un peu plus la victime à coopérer, Cialdini (1993) avance qu'il faut simplement ajouter le mot « parce que » afin de créer l'illusion que la demande est justifiée. Shafir (1993) appuie et avance que dans des situations où un choix est particulièrement difficile à faire en raison d'un haut degré d'incertitude, l'être humain ne prend pas la décision en fonction du choix le plus rationnel, mais en fonction de celui qui est le plus facile à justifier. Dans cette optique, c'est la quantité d'information plutôt que la qualité qui va influencer la cible à coopérer. Par exemple, le pirate donnera plusieurs justifications utiles à la victime afin de prendre la décision qu'il cherche à produire.

Nous construisons notre perception de l'environnement en fonction de nos connaissances et de notre expérience. La perception de ce qui nous entoure influence notre attitude face à une situation ou à une personne. Enfin, c'est notre attitude qui guide nos comportements dans nos actions. Dans cette logique, la perception que les gens ont de la sécurité influence leur attitude et par conséquent, leur comportement vis-à-vis cette dernière. De manière générale, pour un pirate, l'image qu'il projette, au téléphone ou en personne, est très importante, car cela influencera la perception et le comportement de ca cible. Advenant que la cible apprécie le pirate au premier contact, elle sera plus encline à répondre positivement à ses demandes.[3]

1. Réciprocité

La réciprocité est une norme sociale profondément ancrée dans l'humain. Si quelqu'un nous rend un service, on se doit de lui donner quelque chose en retour même si on a rien demandé initialement. Cette technique, connue sous le nom de pied-dans-la-porte, a été étudiée pour la première fois par Freedman et Fraser (1966). Ces derniers voulaient savoir si le simple fait de réaliser un acte des plus anodins (donner l'heure, des directions, signer une pétition) ne nous prédisposait pas à accepter, plus favorablement, une requête ultérieure bien plus coûteuse en temps et en argent (Guéguen, 2004 : 86). Bien que l'acceptation de la requête initiale ne mène pas systématique à l'acceptation de la requête finale, elle augmente considérablement les chances de succès. Le pirate peut utiliser cette technique en commençant par aider la victime concernant un petit problème, sans que celle-ci lui ait demandé de l'aide, ou en donnant un privilège qu'elle n'a pas demandé (Nohlberg, 2009). La victime se sentira alors plus enclin à répondre positivement à une demande ultérieure du pirate afin de lui rendre sa faveur.

Dans le même ordre d'idée, la technique intitulée la porte-dans-le-nez, consiste à commencer par une demande élevée pour ensuite atteindre un niveau de base (Guéguen, 2004 : 119). Cette technique est très utilisée en vente et se base sur le principe de la concession réciproque (Cialdini, 1993). En fait, l'importance n'est pas tant le prix que la concession qui est faite. Cette norme de réciprocité implique que l'on ferait des concessions à ceux qui nous en ont faites.

2. Engagement et cohérence

L'engagement est le lien qui unit l'individu à ses actes. En s'engageant, on active une pression psychologique qui nous mène à accomplir ce que l'on s'est engagé à faire. Cet engagement peut être imposé sans même que le sujet ait son mot à dire. L'engagement active une responsabilité chez les individus à tout faire afin de respecter l'engagement initial. Il est plus efficace lorsqu'il est fait en public ou formellement écrit parce que l'image que l'on projette de soi-même nous incite à respecter notre engagement.

La cohérence dans les actions et les paroles est considérée comme une preuve d'intelligence.

Celui qui change constamment de point de vue n'est pas cohérent avec lui-même. Cela signifie que l'individu continuera à agir en fonction de son engagement initial même si le contexte change. Par exemple, si un inconnu demande à quelqu'un de surveiller son sac alors qu'il va à la toilette et qu'un voleur tente de s'emparer de ce sac, la personne chargée de la surveillance interviendra avec plus de conviction auprès du voleur qui si elle ne s'était pas engagée formellement à surveiller le sac de la personne. Tout cela pour respecter son engagement initial.

Il y a une persistance dans le temps de l'engagement car il est généralement mal vu de changer d'idée. Il est difficile de convaincre un individu avec des menaces ou la violence. Pour le pirate, il est beaucoup plus efficace de convaincre la cible et de l'amener à s'engager à effectuer une tâche.

3. Preuve sociale

Dans l'incertitude, un individu reproduit le comportement du plus grand nombre, s'appuyant sur l'hypothèse que si beaucoup le font, alors c'est bien. Dans ce principe, plus de gens croient qu'une idée est correcte, plus l'idée sera correcte. Ce phénomène, observable dans une multitude de situations, peut avoir un impact important en matière de sécurité, car les membres d'une entreprise vont adapter leur comportement à l'attitude générale de l'organisation face à la sécurité. Si l'attitude générale est que la sécurité peut être négligée alors tout le monde agira de cette manière. Un pirate va utiliser cette technique de persuasion en disant à sa cible que tout le monde le fait donc pourquoi ne pas le faire. Par exemple, tout le monde partage son mot de passe ou prête leur carte d'accès donc pourquoi je ne le ferais pas. Ce type de phénomène engendre une sorte de conformité où ceux qui ne s'y rattachent pas sont identifiés comme ne faisant pas partie du groupe.

4. Autorité

Très jeune, on apprend à répondre positivement à l'autorité, car on réalise qu'il y a des bénéfices à la respecter. L'étude de Stanley Milgram (1974), Obédience to Authority, concernant la soumission, est l'une des figures de l'efficacité de l'autorité les plus célèbres. Plusieurs facteurs viennent influencer ce que l'on perçoit comme une autorité. Il peut s'agir d'uniformes (police, docteur, armée, électricien, maintenance, complet très luxueux), de titres professionnels, d'accessoires (voiture de luxe, cellulaire) ou l'utilisation d'un jargon très précis à un domaine (Cialdini, 1993). L'utilisation de ces symboles d'autorité influence fortement la prise de décision même qu'elle enclenche plus souvent qu'autrement des automatismes. Afin de projeter une image d'autorité, le pirate utilise régulièrement ces instruments de manipulation.

5. Rareté

La rareté augmente la demande pour un produit ou un service. Pour la majorité des gens, ce qui est peu disponible a plus de valeur que ce que l'on trouve un peu partout. Le facteur temps pousse souvent les gens à prendre des décisions moins réfléchies. La rareté fonctionne parce que l'on croit toujours que les bonnes choses sont rares. La rareté est souvent utilisée afin d'offrir un service, mais que la décision doit être prise maintenant, car des facteurs externes font qu'il ne sera plus disponible plus tard. Par exemple, le pirate va demander à la cible de prendre une décision rapidement, car il doit partir.

6. Lien et similarité

Les gens aiment les personnes qui leur ressemblent. Si le pirate présente des similarités avec sa cible, cette dernière sera plus encline à répondre positivement à ses demandes. Le pirate peut demander d'où la cible vient, pour ensuite dire que sa femme vient du même endroit. Il peut aussi créer un ennemi, par exemple le patron, afin d'établir un contact. Un autre phénomène intéressant est l'apparence physique d'une personne. Lorsque l'on voit une personne qui a une apparence attirante, on a tendance à croire que tous ses traits de sa personnalité sont égaux à son apparence. Ce phénomène est appelé l'effet « halo ». Dans les faits, on a tendance à croire qu'une personne qui a une belle apparence est plus honnête, plus intelligente, plus forte, plus

aimable que la normale. Bref, quelqu'un qui a une belle apparence peut plus facilement manipuler les gens.

Conclusion

En conclusion, l'humain est vulnérable au point de vue cognitif, car son jugement est basé sur des biais de raisonnement et au point de vue social, car l'activation de certaines normes sociales influence sa prise de décision. L'ingénierie sociale attaque l'élément vulnérable de la chaîne de sécurité. Ce type d'attaque est particulièrement difficile à contrer. Cependant, l'une des solutions se trouve dans une prise de conscience de ce risque ainsi que dans la compréhension du phénomène et des vulnérabilités qu'il exploite. La formation et la sensibilisation des employés sont des étapes essentielles pour lutter contre l'ingénierie sociale.[3]

Chapitre3 : La mise en pratique de l'ingénierie sociale

Introduction :

Pour prouver que les techniques d'ingénierie sociale peuvent être efficaces autant que d'autres, nous avons essayés dans ce chapitre en premier temps d'évaluer le niveau de vigilance de nos collègues ainsi que nos enseignants à travers un sondage. En deuxième temps, nous avons essayés à travers la tentation de piéger les internautes afin qu'ils nous dévoilent une partie de leurs informations personnels.

I- La première démarche « sondage » :

Dans ce sondage on a posé douze questions auprès des enseignants et des étudiants de notre département d'informatique, le nombre de personnes questionnés est 43. L'objective de ce sondage est de voir qu'elles sont les mauvais comportements qu'un pirate utilisant le sociale engineering peut exploiter. Les questions du sondage étaient focalisées sur les habitudes d'internautes lors du travail sur le web. Nous allons maintenant voir le détailles des réponses et qu'elles sont les remarques à tirer.

Q1) : Vous utilisez un seul mot de passe pour vos compte.
« Messagerie, réseau sociaux, facebook,twiter……. » ?

	Nbr	**Pr%**
Oui	**17**	**39.53**
Non	**26**	**60.46**

-En remarque que 60%Personnes questionnés utilise plusieurs mots de passe pour leurs comptes sur le net. Il y a des gens par peur d'oublier leur mots de passe ils utilisent un seul mot de passe pour tous les comptes, mais, cette habitude peut être une vrai opportunité pour un pirate.

Q2) : Vos mots passe son-il construit à partir des noms de votre entourage « vos enfants, parents, amis…… » ?.

	Nbr	**Pr**
Oui	**19**	**44.18**
Non	**24**	**55.81**

-Les gens montrent leurs affections envers leurs enfants par exemples, en utilisant leurs noms comme des mots de passe et cela présente une vulnérabilité. Lors du sondage, on a remarqué que même des enseignants qui sont sensés plus soucieux et mieux informées utilisent les noms de leurs enfants et parents dans leurs mots de passe.

Q3) : Lorsque vous recevez des spams, et-ce-que vous être tenté à les ouvrir ?

	Nbr	**Pr%**
Oui	**17**	**39.53**
Non	**26**	**60.46**

-En remarque que les personnes questionnés n'ouvre pas les spams, car ils ne font pas confiance au contenu de ces spams. Par curiosité, ou par ignorance certains internautes ouvrent les spams. Et c'est bien ce que font les grands entreprises, ils utilisent les spams afin de passer leurs publicités sur le net.

Q4) : Faits-vous confiance à votre service de messagerie ?

	Nbr	**Pr%**
Oui	**22**	**51.13**
Non	**21**	**48.83**

-les personnes questionnés sont partagés entre les confiants et non confiants à un pourcentage de50%.

Q5) :Utilisez-vous votre propre identité pour crier vos différents comptes ?

	Nbr	**Pr%**
Oui	**27**	**62.79**
Non	**16**	**37.20**

-La plus part des personnes questionnés utilise leur propre identités pour la création des différente comptes. C'est un comportement dangereux surtout si on détient des informations sensibles. En plus, cela aide le pirate à bien connaitre l'individu derrière.

Q6) : Si votre anti-virus vous alerte un site dangereux, vous ignorez les recommandations de l'antivirus ?

	Nbr	**Pr%**
Oui	**17**	**39.53**
Non	**26**	**60.46**

-60%des personnes questionnés faite confiance à l'antivirus et leurs recommandations.

Q7) : pouvez-vous être une cible pour un pirate ?

	Nbr	**Pr%**
Oui	**19**	**44.18**
Non	**24**	**55.81**

-50%des personnes sentent qu'ils sont une cible pour des pirates du web.

Q8) :Fait-vous des relations avec des inconnus sur internet ?

	Nbr	**Pr%**
Oui	**19**	**44.18**
Non	**24**	**55.81**

-La moitié de personnes questionnées faites des relations avec des inconnus sur internet. Il faut savoir que les forums sont les meilleurs lieux convoités par les pirates pour tisser des relations d'amitié avec leurs cibles.

Q9) : Est-ce-que, vous pouvez partager votre mot de passe avec vos proches ?

	Nbr	**Pr%**
Oui	**16**	**37.20**
Non	**27**	**62.79**

-Un grand pourcentage des personnes ne partage pas leurs mots de passe avec des proches.

Q10) :pouvez-vous partager vos informations « photos, vidéos…… »Avec des inconnus ?

	Nbr	**Pr%**
Oui	**14**	**32.55**
Non	**29**	**67.44**

-68% des personnes ne partage pas leurs informations avec des inconnus. Cette pratique est bien perçu sur les réseaux sociaux, et plus on se montre plus le pirate peut trouver nos faiblesses.

Q11) :Est-ce-que vous utilisez des mots de passe complexes et longs « chiffres, symboles ».@,2,c, &,*…, ou simple et courts ?

	Nbr	**Pr%**
Oui	**25**	**58.13**
Non	**18**	**41.86**

-58% utilise des mots de passe complexe et longs pour protéger leurs comptes.

Q12) : Est-ce-que vous connaissez le terme « ingénierie sociale » ?

	Nbr	**Pr%**
Oui	**8**	**18.60**
Non	**35**	**81.39**

-La majorité de personnes questionnées ne connaissent pas le terme ingénierie sociale.

* Dans ce sondage on a constaté que la plupart de personnes questionnées, sont méfiantes Ils sont bien sécurisés et ceci est positif pour la sécurité informatique

II- La deuxième démarche :

Le rêve d'aller ailleurs pour continuer les études supérieures est toujours omniprésent dans les esprits de nos étudiants. Nous avons joués sur cette faiblesse afin de piéger nos collègues.

Nous avons élaborés un formulaire pour un visa afin de suivre des études en France, ou un séjour qui permet à son détenteur de se présenter à un entretien ou à un concours d'entrée dans un établissement supérieur hautement réputé, suscite pour nos étudiants un vif intérêt et leurs donnera l'opportunité de développer et approfondir les acquis et les connaissances théoriques de ses études, et leurs permettra ainsi d'enrichir et de contribuer à un meilleur développement d'apprentissage dans leur pays d'origine.

Nous avons partagé ce formulaire avec nos collègues de formation notamment nos amis sur Facebook, après avoir créé un compte Yahoo pour qu'ils puissent nous contacter, et nous envoient le formulaire avec leurs informations personnels.

Nous avons aussi laissé intentionnellement dans le formulaire des indices (N° Carte d'identité) que quelqu'un bien avertis peut comprendre que c'est juste une blague.

Voici si dessous le formulaire:

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

RÉPUBLIQUE FRANÇAISE

cerfa
N° 14052*01

DEMANDE DE VISA POUR « ETUDIANT-CONCOURS »

Ce visa permet à son détenteur de se présenter à un entretien ou à un concoure d'entrée dans un établissement d'enseignement supérieur public ou privé. En cas de réussite, l'étudiant peut solliciter, sans retourner dans son pays d'origine, un titre de séjour d'un an renouvelable, à la préfecture.

N°	Libellé
01	**Nom :**
02	**Prénom :**
03	**Date de naissance :**
04	**Lieu de naissance :**
05	**Pays de naissance :**
06	**Nationalité actuelle,** **Nationalité a la naissance,** **Si différente:**
07	**Sexe :**
08	**Numéro de carte d'identité :**
09	**Adresse électronique :**
10	**Numéro de téléphone :**
11	**Formation :**

Veuillez envoyer vos coordonnées dans cette adresse e-mail :

visatudiant@yahoo.fr

1- Résultats de l'expérience

Nous avons constaté malheureusement, que la majorité de nos collègues qui sont normalement sensibilisés à la sécurité plus que les autres étudiants, ont été facilement piégés. Notre démarché n'a pas été bien construite, car nous avons prévus un site web afin de donner plus de crédibilité à notre démarche. Alors, nous avons juste utilisée nos pages personnels sur Facebook et ça a marché comme même.

Dés le premier jour ou on a partagé sur Facebook ce faux visa, on a piégé quatre personnes qui ont renseignés ce par ce faux document par leurs informations personnels, il y avait une seule personne qui s'est rendu compte que ce visa est faux. Et au fil des jours d'autres personnes sont tombés dans le piège et nous avons reçus pas mal de formulaires sur notre faux adresse email.

Finalement, malgré les lacunes perceptibles dans notre démarche, les techniques du l'ingénierie sociale reste une attaque vraiment possible et l'être humain demeure le maillon faible dans n'importe quelle système de sécurité.

III- Recommandations :

1- Enregistrez vos sites de confiance

On dit que la confiance se mérite. Les nouveaux sites sont comme les personnes que l'on rencontre pour la première fois. La confiance n'est pas immédiate.

2- Restez sceptique

Ne cliquez jamais sur des liens suspects, même si le message qui les accompagne est très prometteur. Si c'est trop beau pour être vrai, soyez sur vos gardes.

3- Ne cédez pas a la panique

Ne vous laissez pas intimider par les menaces. Nombre de cybercriminels comptent sur l'élément de surprise pour vous amener à faire quelque chose à votre insu. Mieux vaut ignorer purement et simplement les tactiques basées sur la peur.

4- Faites passer le mot

Partagez ces informations avec votre entourage afin qu'ils adoptent un comportement sans danger. Ne les laissez pas tomber dans les pièges des cybercriminels.

5- Mieux vaut prévenir que guérir

Investissez dans une solution de sécurité efficace qui protège votre système et vos données contre tous les types de menaces. Explorez et utilisez les fonctionnalités de sécurité intégrées aux sites et pages que vous visitez régulièrement. Certains sites comme Facebook vous donnent même des informations sur les dernières menaces et des conseils pour vous aider à naviguer en toute sécurité.

Conclusion :

A travers ces deux exemples réels utilisés nous constatons que la majorité des gens sont une proie facile pour l'ingénierie sociale c'est pour cela il faut que nous serons plus méfiant et vigilant vers les tentations.

Conclusion générale

Même si on parle moins de l'ingénierie sociale que du phishing, il faut être très vigilant et sensibiliser tous les utilisateurs des systèmes d'information dans nos entreprises. Il ne faut pas être paranoïaque, mais n'importe quelle entreprise peut être victime d'une attaque. Et cette attaque sera précédée d'ingénierie sociale afin d'obtenir les renseignements indispensables à cette attaque. Ces renseignements peuvent être de plusieurs ordres : profils, mots de passe, mais aussi anti-virus, navigateurs, logiciels utilisés, etc…

On peut conclure finalement que l'ingénierie sociale est une sorte d'attaque très puissant, pourtant qu'il ne s'appuie pas beaucoup sur des notions informatique.

La consigne doit être de ne donner aucune information concernant le Système d'Information par téléphone quel que soit l'interlocuteur, ou à une personne inconnue rencontrée dans ou hors de l'entreprise. Et un mot de passe ne se donne jamais, même à une personne connue.

Bien sûr, aucun sujet traitant l'ingénierie sociale est complet sans la mention de Kevin Mitnick, l' ancien hacker américain et l'écrivain de livre « L'art de la supercherie », donc je vais conclure avec une citation de lui à partir d'un article paru dans Security Focus :

"Vous pouvez passer d'une technologie et des services d'achat fortune ... et votre infrastructure réseau pourrait demeurent vulnérables à l'ancienne manipulation ".

Bibliographie

[1] : Solange G .,sécurité informatique et réseaux ., 4ème édition .,2006 .,pp.6,7,8,9,10.

[2] : résumé livre : sécurité informatique et réseaux .,pp.3,4,5,6,7.

[3] : David C ., la cadre du cours CRI-6234, « Nouvelles technologies et crimes » (session d'automne 2009).

[4] : réseaux-ch-10 .,8 novembre 2006 .,pp.4,5,6.

Webographie

[5] : http://www.pearson.fr/resource/.download.cfm?/…réseaux -ch-10.pdf,consulté le 26 février 2014.

[6] : http://www.ducrot.org/securite.pdf , consulté le 2 mars 2014.

[7] : https://www.cases.lu/ingenierie-sociale.html, consulté le 10 mars 2014

Annexe1 : Étude de cas

Celui qui attaque, se décrit comme étant en charge du réseau informatique devant résoudre et

enquêter sur des problèmes critiques concernant le réseau informatique. Il téléphone et s'introduit à la cible. Il remarque son accent et lui demande d'où il vient. Selon la réponse, il invente minutes (lien et similarité) que sa femme vient de la même ville. Ils échangent pendant quelques sur la région ou leur relation familiale.

Ensuite, il demande à la cible si elle peut passer du temps avec lui pour réparer le réseau (engagement). Il commence à décrire le problème du réseau en utilisant un jargon très technique (autorité). Il lui vulgarise que les ordinateurs portables doivent être retirés du système pour quelques jours afin de les nettoyer. Il ajoute que chaque ordinateur devra être apporté au bureau de son entreprise afin d'être réparé. Il ajoute que plusieurs de ses collègues ont le même problème (preuve sociale) et qu'ils devront passer par le même processus au cours des prochains jours. Il continue en lui donnant plusieurs informations très techniques (surcharge d'information).

Par la suite, il lui fait une faveur (réciprocité), en lui disant qu'il peut régler le problème pour que

la cible ne perde pas trop de temps. Mais l'attaquant a un délai de temps très restreint, car il doit partir en vacances (rareté) à la fin de la journée. Avant de partir, il aimerait bien avoir terminé, cette section du réseau de l'entreprise. Cependant, s'il respecte la procédure établie entre les deux compagnies, il ne pourra jamais terminer avant de partir et son patron sera mécontent.

La cible doit faire une petite faveur (réciprocité) en ne parlant de cela à personne, car l'attaquant pourrait perdre son travail à cause de la sévérité de son patron (lien et similarité). Il discute pendant quelques minutes sur le caractère des gestionnaires.

Il dit à la cible que le moyen le plus rapide de régler son problème est d'apporter son portable au bureau fictif de l'attaquant qui est situé à 15 minutes de voiture. Il lui mentionne qu'il doit apporter des pièces d'identité photo. Ensuite il lui décrit la procédure à suivre, il faut une lettre signée d'un collègue, les papiers de son ordinateur et un historique détaillé des opérations effectuées sur l'ordinateur lors de la dernière année. Toute cette procédure est une exigence de sa compagnie (celle du fraudeur), une sorte de police d'assurance pour sa firme, mais que la compagnie de la cible n'a aucun intérêt à émettre tous ces papiers. Si la cible le veut bien, il lui offre de garder cela entre eux, la cible aurait juste à donner son nom d'utilisateur et son mot de passe.

Il s'agit d'un exemple simple et classique d'ingénierie sociale. Selon la cible, en utilisant les bonnes circonstances, ces attaques peuvent être très efficaces.

L'une des attaques les plus fréquentes est de simplement attendre à l'extérieur de l'édifice ciblé,

L'attaquant peut également se présenter à l'entrée des employées avec plusieurs boîtes et simplement demander à un employé légitime de lui ouvrir la porte.

Ces techniques très simples permettent de contrer bien des investissements technologiques en exploitant simplement la bonne volonté des gens.