Le *social engineering* :
Un risque sous-évalué du système d'information de l'entreprise moderne

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES en Informatique de Gestion

par :

Mirco BONIOLO

Conseiller au travail de Bachelor :

Peter DAEHNE, Professeur HES

Genève, le 25 juin 2013

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de gestion

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre Bachelor of Science en Informatique de gestion. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Genève, le 25 juin 2013

Mirco BONIOLO

Remerciements

Je tiens ici à adresser mes plus sincères remerciements à mon conseiller au travail de Bachelor, M. Peter DAEHNE, qui m'a suivi tout au long de ce travail et s'est toujours montrée disponible pour répondre à mes questions. Ses remarques, ses réflexions et nos nombreuses entrevues m'ont permis d'aboutir au présent rapport.

Un merci également aux bibliothécaires de l'Université de Montréal, qui m'ont aidé dans mes diverses recherches documentaires et les commandes des différents articles scientifiques auxquels j'ai pu accéder par leurs soins.

Pour finir, je tiens aussi à adresser mes chaleureux remerciements à ma famille, mes proches et mes amis, qui m'ont soutenu tout au long de ce projet.

Résumé

Le *social engineering* est un risque dont la prise de conscience est relativement récente du point de vue de la sécurité des systèmes d'information. Il constitue donc un objet d'étude de premier choix pour celles et ceux qui s'intéressent aux risques informatiques pesant sur le système d'information ou qui doivent les gérer et amener des solutions concrètes.

Nous avons commencé ici par nous informer sur cette menace et notamment pour mettre une définition claire sur ce concept multiforme. En effet comprendre le risque, c'est d'abord en saisir ses contours. Nous poursuivons ensuite sur ses caractéristiques, ses spécificités. Des outils et modèles sont proposés pour le traitement et la mitigation.

Le premier constat est que cette menace reste très fortement sous-évaluée. Avec 41% des professionnels de la sécurité sondés qui ne savent pas s'ils ont été la cible ou non de ce type de risque, il est important de comprendre ce phénomène. Deuxièmement, un manque de formation et de sensibilisation du personnel vis-à-vis de ce risque nous sont clairement apparus au fur et à mesure de notre travail (26% seulement ont mis en place un programme de sensibilisation). Troisième point, la valeur de l'information n'est pas toujours prise en considération. Enfin, les nouvelles technologies du Web exacerbent ce type de phénomène.

Table des matières

Déclaration i
Remerciements ii
Résumé iii
Table des matières iv
Liste des Tableaux vi
Liste des Figures vi
1. Introduction 1
1.1 Tour d'horizon du problème 1
1.2 Le périmètre de notre recherche 2
1.3 La méthodologie du travail de recherche 3
2. Une définition 4
2.1 Le social engineering qu'est-ce que c'est? 4
2.2 Un état de l'art 6
3. Les quatre étapes d'une attaque d'ingénierie sociale 14
3.1 Une approche globale 14
3.2 La récolte d'information 16
3.3 Le prétexte 18
3.3.1 Les biais cognitifs *19*
3.4 L'extraction 31
3.5 La clôture 32
4. Techniques et outils pour l'ingénierie sociale 33
4.1 Les réseaux sociaux et le Web en général 33
4.1.1 Une politique pour encadrer *36*
4.1.1.1 Facebook, Twitter et compagnie 42
4.2 Les moteurs de recherche 45
4.3 Techniques courantes 50
5. Formation, prévention et mitigation 61
5.1 La formation et la sensibilisation des employés 61
5.2 La sensibilisation à tous les niveaux 64
5.3 Les moyens de mitigation 65
5.4 Tests d'intrusion et audits 68
6. L'entreprise moderne comme catalyseur 73
6.1 La gestion de l'information 73
6.1.1 Les débuts d'une politique de l'information *76*
6.2 Social engineering et politique de sécurité 80
7. Conclusion 82
7.1 Synthèse du travail de recherche 82
7.2 Un apport personnel 83

Glossaire **85**

Bibliographie **90**

Livres (monographies) : **90**
Articles de périodique : **90**
Articles de conférences : **91**
Articles électroniques : **91**
Pages Web : **92**
Norme : **92**

Annexe 1 Exemples d'attaques de *social engineering* **93**

Annexe 2 Deux exemples de biais supplémentaire **96**

Liste des Tableaux

Tableau 1 Chiffres clés sur l'état de l'art du *social engineering* 12

Tableau 2 Exemples de lignes directrices générales 38

Tableau 3 Lignes directrices relatives aux contenus postés par les employés 39

Tableau 4 Lignes directrices pour le comportement en ligne 40

Tableau 5 Exemples de lignes directrices à l'attention du public 41

Tableau 6 Requêtes combinées pour la recherche d'informations sous *Google* 47

Liste des Figures

Figure 1 Les composantes de la définition du *social engineering* 4

Figure 2 Liste des principaux facteurs motivationnels cités pour une attaque 8

Figure 3 Typologie et probabilité du personnel à risque 9

Figure 4 Approches diverses liées au *social engineering* en entreprise 10

Figure 5 Les quatre étapes d'une attaque de *social engineering*……. 16

Figure 6 Exemples d'opérateurs pour la recherche d'informations sous *Google* 46

Figure 7 Exemples d'informations récoltées via la recherche passive 48

Figure 8 Liste des principales techniques d'ingénierie sociale 51

Figure 9 Human security – the missing link 69

Figure 10 La fuite d'information dans le domaine publique en entreprise 74

1. Introduction

1.1 Tour d'horizon du problème

Dans l'entreprise moderne, la gestion du risque au sens large du terme est devenu un élément quasi incontournable de sa stratégie. Que ce soit pour gérer et protéger ses actifs informationnels et ses biens physiques, ou encore pour se créer de nouvelles opportunités sur des marchés, tout en pérennisant ses activités métier sur le long terme. Dès lors, les entreprises ont pris pour habitude de se préoccuper de toutes une série d'éléments bien connus comme le risque sur les opérations (risque opérationnel), le risque de réputation (ou risque d'image), le risque d'intrusion physique (virus, chevaux de Troie, …), ou encore le risque de catastrophe naturelle.

De la PME à la grande entreprise travaillant à l'international, des procédures sont mises en place et des systèmes de contrôle et d'audit (interne ou externe) permettent de suivre et de vérifier régulièrement la conformité des règles établies avec l'intégrité du système d'information. Le système d'information est aujourd'hui devenu une ressource clé des entreprises. Ajoutons également que les progrès de la technique moderne nous fournissent des outils de plus en plus puissants, fiables et difficiles à contourner comme par exemple : le firewall, les systèmes de détection d'intrusions, les logiciels antivirus, les systèmes cryptographiques (cf. glossaire p.85 pour plus de détails sur les termes) etc. Ces derniers ont sans aucun doute amené des bénéfices certains dans la gestion et la protection des données, mais il serait faux de croire que l'on peut se barricader derrière ces systèmes pour garantir une sécurité sans faille.

En effet, depuis toujours, le maillon faible de tout système de sécurité est précisément celui qui en détient les commandes, c'est-à-dire l'humain lui-même. Depuis maintenant environ une dizaine d'années, nous voyons apparaître un nouveau risque pour le système d'information des entreprises. Ce risque s'appelle le *social engineering* ou risque d'ingénierie sociale. Il ne s'agit plus dès lors de directement s'attaquer à la partie technique du système d'information informatisé comme le ferait un pirate conventionnel, mais bel et bien de prendre pour cible les personnes qui se trouvent derrière leurs machines et leur réseau ultra-sécurisé. Le pirate moderne va alors mêler techniques informatiques, compétences sociales et éléments de psychologie humaine pour parvenir à ses fins. Ce risque reste méconnu à plus d'un titre : d'une part parce qu'il est relativement nouveau, et d'autre part, du fait de sa nature particulière (il n'est pas un risque relevant uniquement d'habiletés techniques) ; il est presque toujours sous-estimé et peu pris en considération par le management. Il passe alors le plus

souvent sous le radar des équipes de sécurité. De surcroît, il existe peu d'éléments statistiques qui concernent ce domaine. Voilà comment nous obtenons l'une des menaces les plus sérieuses sur le système informationnel de l'entreprise contemporaine. Comme nous le verrons dans la suite de notre recherche, le *social engineering* est une menace qui doit être prise au sérieux et qui peut causer de gros dégâts, au même titre que les attaques dites conventionnelles.

L'homme devient alors simultanément le point faible, mais également le point fort de la sécurité du système d'information. Car il peut se montrer adaptatif, évolutif et apprendre à détecter la supercherie là où une machine ne le peut pas.

1.2 Le périmètre de notre recherche

De manière à établir un périmètre clair pour notre recherche, voici la problématique et les questions de recherche auxquelles nous nous proposons de répondre.

La problématique :

Les actifs informationnels et leur sécurisation sont devenus l'un des piliers de la stratégie d'entreprise. Le problème que nous nous proposons d'étudier ici est :

Comment l'entreprise moderne peut et doit sécuriser son système d'information (informatisé ou non) à l'externe comme à l'interne, sous l'angle de la menace du social engineering, tout en lui conférant une perméabilité sélective de l'information?

Les questions de recherche :

Les questions qui se posent et que nous pouvons identifier à partir du problème susmentionné sont alors :

- Comment former et éduquer le personnel à ce type de menace?
- Quelles sont les contremesures et les moyens de mitigation que l'on peut mettre en place?
- Quelle est la place qu'occupe une politique de l'information au sein de la politique de sécurité globale de l'entreprise?
- Comment les médias sociaux et la démocratisation du Web sont-ils devenus des catalyseurs de ce type de risque, par l'entrecroisement des sphères professionnelles et privées?

1.3 La méthodologie du travail de recherche

Pour mener ce travail à bien et répondre aux diverses questions que nous nous posons, il s'agit en premier lieu de cerner de façon précise le risque auquel nous faisons face. Nous commencerons donc par définir ce dernier afin de déterminer sa typologie et ses spécificités. Comme nous le verrons, du fait de sa nature ambivalente et versatile, il existe plusieurs définitions du phénomène. Nous tenterons ensuite de faire un état de l'art du risque considéré et nous poursuivrons en expliquant et illustrant les grandes étapes d'une attaque de *social engineering*.

Le travail sera découpé à partir de ce moment là en cinq grands axes de recherche :

1. Les techniques et outils d'ingénierie sociale
2. La formation et l'éducation du personnel
3. Les contremesures et moyens de mitigation possibles
4. Les médias sociaux et le Web
5. La politique de l'information dans un contexte global de sécurité d'entreprise

Nous terminerons par une synthèse mentionnant une série de recommandations, les principaux enseignements que nous pouvons tirer de notre analyse et une conclusion.

Nous avons été amenés à consulter bon nombre de sources diverses telle que :

- Des sites spécialisés dans l'audit de la sécurité
- Des articles de conférences sur la sécurité informatique
- Des lexiques et encyclopédies
- Des magazines scientifiques traitant du domaine de la sécurité de l'information
- Des ouvrages spécialisés

Dans un souci de fiabilité, de qualité et d'exactitude de nos sources et informations présentées, nous nous sommes efforcées tant que possible de ne choisir que des articles, documents, etc. ne remontant à pas plus de cinq ou six ans.

2. Une définition

2.1 *Le social engineering qu'est-ce que c'est?*

Du fait de sa nature particulière, le *social engineering* n'est pas un risque conventionnel, c'est-à-dire faisant appel aux seules compétences techniques du pirate. Il combine deux dimensions distinctes et complémentaires: un aspect qui fait appel aux compétences sociales et humaines de l'individu et un aspect qui fait appel à des compétences plus techniques. Dès lors, nous pouvons comprendre que mettre une définition sur ce concept n'est pas toujours chose aisée. Il existe alors plusieurs définitions du phénomène. Toutes les définitions, que nous avons pu obtenir dans la littérature s'accordent toutefois sur les éléments suivants en entrée et en sortie :

- ***Entrée:*** compétences humaines et sociales, habiletés psychologiques, biais cognitifs & compétences techniques
- ***Sortie:*** système d'information, information stratégique & bien ou information convoités

Ce qui, d'un point de vue schématique, peut se représenter de la manière suivante :

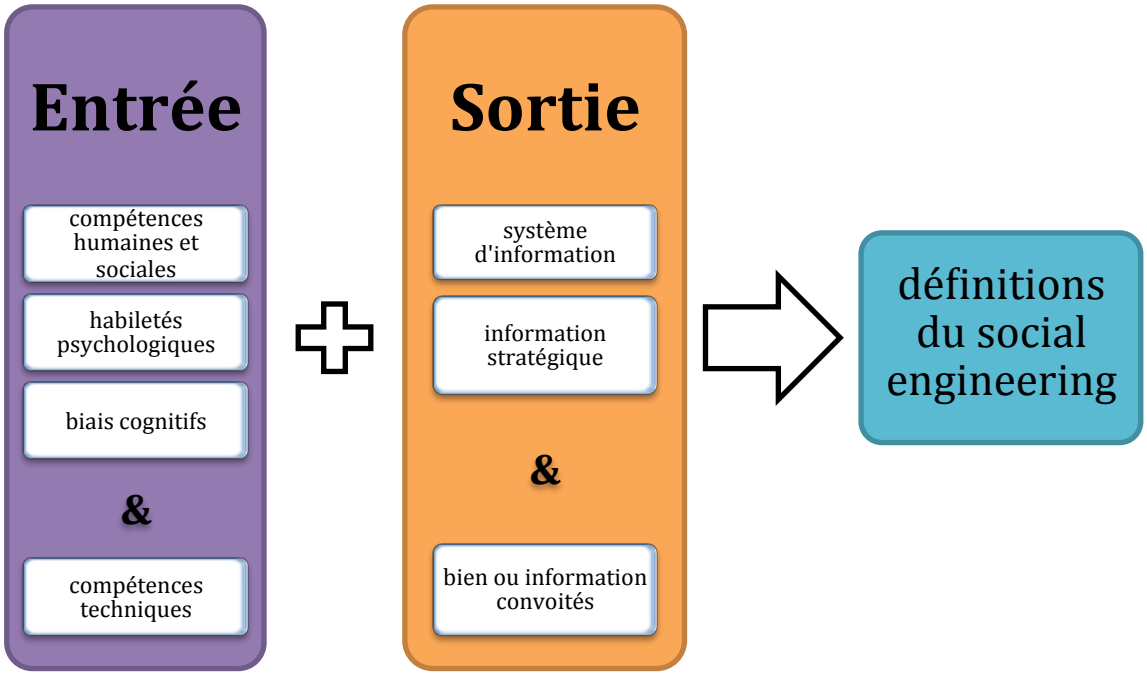


Figure 1 - Les composantes de la définition du *social engineering*. Toutes les définitions font appels à ces divers éléments pour donner une explication du phénomène.

Nous nous proposons de donner ici trois définitions possibles tirées directement du lexique du renseignement de M. Jacquet [1] :

> *« L'ensemble des techniques de manipulation qui conduisent à convaincre quelqu'un d'effectuer de son plein gré une transgression ou une divulgation d'informations confidentielles. Il s'agit d'obtenir quelque chose (un bien ou une information) en exploitant la confiance, mais parfois également l'ignorance ou la crédulité de tierces personnes, pour obtenir un accès à un système informatique. »*
>
> *« Aussi appelé élicitation, le social engineering est une technique qui a pour but d'extirper frauduleusement des informations à autrui. »*
>
> *« Il peut aussi se définir comme l'art de se servir des failles humaines afin d'obtenir de son interlocuteur, par des moyens détournés ou indirects, mais toujours déloyaux, des informations qu'il ne souhaitait pas ou n'était pas autorisé à divulguer. Information sensible et stratégique. »*

À partir des diverses lectures que nous avons effectuées et de nos divers recoupements, nous pouvons ici donner notre propre définition du phénomène :

> *« Le social engineering ou ingénierie sociale est un ensemble de méthodes et de techniques de manipulation psychologique humaines (charisme, persuasion, savoir mentir, etc.) permettant au travers d'une approche relationnelle basée sur l'influence, la manipulation, la serviabilité, la confiance et la bonne foi, d'obtenir l'accès à un système d'information ou à des informations à haute valeur stratégique. »*

Comme nous pouvons le voir dans ces définitions, c'est justement ces multiples facettes, cette versatilité de ce risque bien particulier qui le rend si dangereux et si difficile à détecter. En effet, à partir du moment où la manipulation psychologique d'un individu entre en jeu, il est très difficile de se rendre compte, pour celui qui est manipulé, qu'il est précisément sous l'emprise d'un ingénieur social.

La question que nous pouvons alors nous poser est celle de savoir quelle est la part, le poids des compétences humaines et sociales versus celles techniques? Bien qu'il soit difficile de pouvoir chiffrer, quantifier le poids de chacun des aspects dans ces définitions, et donc le rôle que l'un et l'autre jouent dans l'avènement de ces pirates des temps modernes, il est clair que l'aspect social est la clé de voûte de ce nouveau type de risque. En effet, le hacker n'a plus nécessairement besoin d'être un as de l'informatique pour forcer réseaux sécurisés, coffre-forts et autres systèmes cryptés, puisque ce dernier manipule autrui pour arriver à ses fins. Il peut dès lors s'affranchir de compétences techniques pointues et se concentrer sur la manipulation.

---

1 JACQUET, Laurent. *Lexique du renseignement, de l'information et de l'influence*. L'Esprit du Livre Editions. Paris : 2010, pp.102-103

Les compétences techniques deviennent alors un atout, un outil au service de l'attaque d'ingénierie sociale. Une connaissance accrue des processus et de la cible dans son ensemble va lui conférer une puissance supplémentaire pour affiner, ajuster son scénario d'attaque.

Nous terminerons en disant que certains le considèrent comme le piratage du cerveau humain.

2.2 Un état de l'art

Établir un état de l'art dans ce domaine n'est pas chose aisée et cela à plus d'un titre. En effet, comme nous l'avons exposé en préambule, ce phénomène étant relativement peu pris en considération, voir même fortement sous-estimé par les entreprises modernes dans leur stratégie de gestion des risques, peu de statistiques existent sur le sujet. Parmi les éléments qui expliquent cette carence, nous pouvons notamment citer les trois raisons principales suivantes :

- Ce risque étant sous-évalué, une très grande majorité des entreprises n'ont purement et simplement pas conscience du phénomène et de son éventuel impact sur leurs activités entrepreneuriales.
- Ce thème n'étant que très rarement intégré dans l'outil de gestion des risques, la grande majorité des entreprises qui font l'objet de sondages en matière de sécurité ne sont dès lors pas capables de déterminer si elles ont ou non été la cible de ce phénomène.
- Les entreprises qui sont les cibles de ce type de pirate sont généralement de grands groupes internationaux ou actives dans le secteur tertiaire[2] comme par exemple : banques, assurances, télécommunications etc. Dès lors, ce type d'information n'est pas publié pour des questions d'image et de concurrence accrue entre les différents acteurs de ces marchés. La publication de telles informations reviendrait à divulguer les faiblesses potentielles d'un système, ce qui n'est purement et simplement pas imaginable.

Malgré ces difficultés, nous avons voulu essayer de donner quelques chiffres clés pour tenter d'établir, si ce n'est un point précis, au moins un tour d'horizon. Le sondage sur lequel nous nous basons ici pour notre analyse est directement tiré d'une étude de marché effectué en septembre 2011 par la société *Dimensional Research* sur mandat

2 Biens et services

de *Check Point Software Technologies LTD*[3]. La première est spécialisée dans la conduite d'études de marchés (essentiellement des études marketing pour les professionnels opérant dans les TIC[4]) ; quant à la deuxième, elle développe notamment des solutions logicielles pour la sécurité informatique. L'étude a été menée auprès de 853 sondés, dans 6 pays (Etats-Unis, Grande-Bretagne, Canada, Australie, Nouvelle-Zélande et Allemagne) durant la période de juillet à août de l'année susmentionnée. Précisions que les entreprises sondées sont actives dans tous les secteurs d'activités et que la taille varie de la petite structure (moins de 100 employés) à l'entreprise multinationale (plus de 15'000 employés). Enfin, le profil des répondants est essentiellement celui de professionnels travaillant dans les TIC et dont la part essentielle du travail consiste à garantir la sécurité des systèmes d'informations de ces entités. Il s'agit par exemple de cadres et de directeurs de l'informatique, mais aussi d'informaticiens sur le terrain chargés d'appliquer les mesures et les politiques de sécurité mises en place.

Une première constatation en demi-teinte est que parmi les professionnels de la sécurité (c'est-à-dire ceux dont la sécurité représente l'entier de leur travail ou une part non négligeable de leur activité professionnelle quotidienne), 35% ont conscience de la menace d'ingénierie sociale. Et 62% admettent en avoir hautement conscience comme étant un risque potentiellement sérieux. Contre respectivement 39% (conscience) et 47% (hautement conscience) pour l'ensemble des professionnels de l'informatique sondés[5].

Sur l'ensemble des participants, 43% ont indiqué que leur entreprise a déjà fait face à ce type d'attaque contre 41% d'entre eux qui ne peuvent se prononcer sur la survenue ou non d'un telle menace.

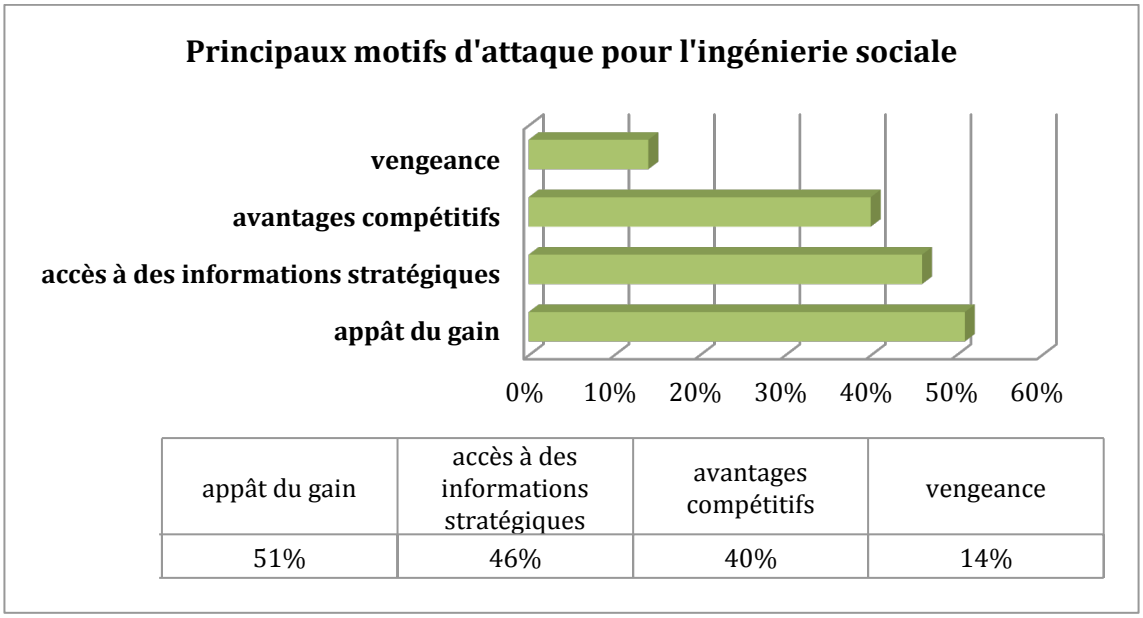
Un autre fait intéressant concerne la (les) motivation(s) liée(s) à ce phénomène. La Figure 2 ci-après représente, d'après le pourcentage des sondés ayant indiqué avoir été victime de ce type d'attaque (les 43% ci-dessus), et selon leur ordre d'importance, les principaux motifs d'attaque.

---

3 *The risk of social engineering on information security :* A survey of IT professionals http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf

4 Technologies de l'information et de la communication

5 Lors de cette étude, les participants ont été invités à évaluer leur niveau de conscience de la menace d'ingénierie sociale comme risque de sécurité potentiel. Les valeurs possibles étaient : très conscient (*highly aware*), conscient (*aware*), peu conscient (*somewhat aware*), jamais entendu parler (*never heard of it*).



appât du gain	accès à des informations stratégiques	avantages compétitifs	vengeance
51%	46%	40%	14%

Figure 2 – Liste des principaux facteurs motivationnels cités pour une attaque. Le pourcentage indique la fréquence d'occurrence de chacun des motifs auprès du pourcentage des sondés (43%) ayant indiqué que leur entreprise a déjà fait face à cette menace. Par exemple. : 51% d'entre eux ont signifié l'appât du gain comme motif etc.

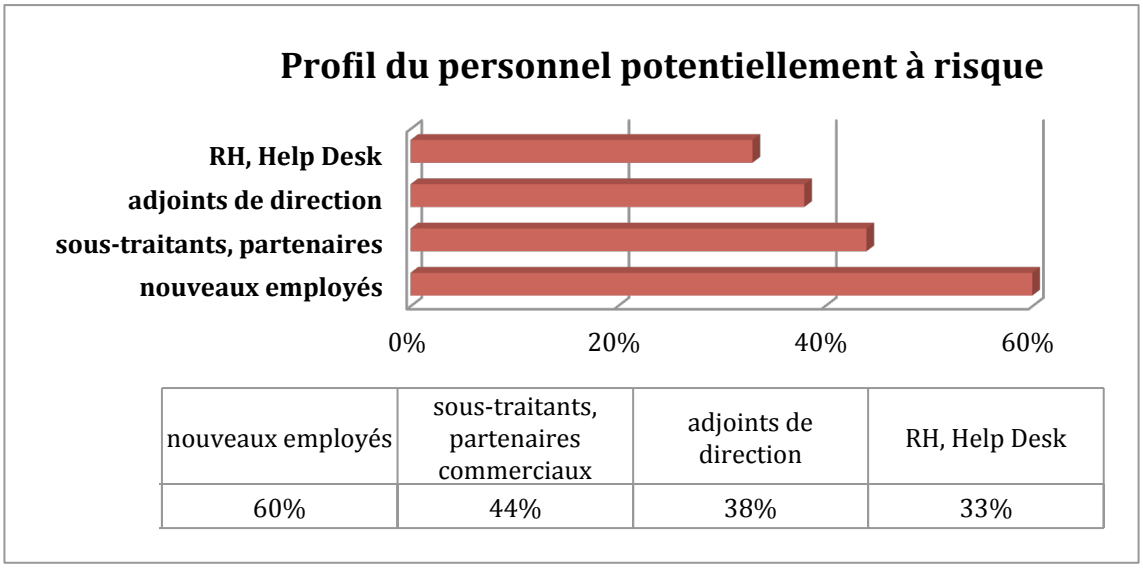
Sur les 853 sondés de départ, 322 ont indiqué avoir subi de telles attaques et effectué un reporting systématique (ce qui représente environ 37%). Parmi les entreprises de plus de 5'000 employés 48% ont fait état de 25 ou plus attaques de *social engineering* au cours des deux dernières années. Enfin, 56% de toutes les compagnies (toutes tailles confondues) indiquent avoir subi entre 5 et 25 attaques au cours de la même période.

Toujours sur ces 322 répondants, il leur a été demandé quel était le coût moyen[6] (c'est-à-dire la perte moyenne) lié à l'attaque subie. 30% des entreprises de plus de 5'000 employés ont indiqué un coût moyen par incident de plus de 100'000 dollars US. Et 48 pourcent des entreprises toutes tailles confondues, un coût moyen de 25'000 dollars US.

La typologie des employés est également un élément important à prendre en compte dans le scénario global d'une attaque. En effet, en fonction du « type » d'employé, il sera plus ou moins facile par le pirate de créer une brèche exploitable pour accéder ultérieurement au contenu désiré. C'est pourquoi, l'étude s'est également intéressée à savoir quel était le profil du personnel le plus susceptible de donner lieu à une faille de

6 Le coût comprend entre autre les éléments suivants : l'interruption éventuelle de l'activité, les dépenses clients, la perte sur le chiffre d'affaire, la main d'œuvre.

sécurité. La question « quel est le type de personnel le plus à risque? » a été posée auprès de l'ensemble des sondés (853 au total). Il en ressort les éléments suivants :



nouveaux employés	sous-traitants, partenaires commerciaux	adjoints de direction	RH, Help Desk
60%	44%	38%	33%

Figure 3 - Typologie et probabilité du personnel à risque. Les pourcentages indiquent la probabilité qu'un certain type de personnel soit plus à même d'être pris pour cible par un ingénieur sociale. Par exemple: 60% sont des nouveaux employés etc.

En ce qui concerne les nouveaux employés, il est aisé de comprendre le risque potentiel que ceux-ci représentent. De part leur méconnaissance des procédures, du cadre de travail nouveau etc., il est relativement facile de se laisser éventuellement berner et de fournir à peu près à n'importe qui de bonne foi ou soit disant de bonne intention des informations plus ou moins importantes. Ceci est d'autant plus vrai lorsqu'ils ne connaissent pas encore bien les rouages et les personnes de l'entreprise.

Pour les entrepreneurs et sous-traitants, nous pouvons soulever l'argument d'une moins bonne connaissance de la politique de sécurité interne de l'entreprise avec laquelle ils sont en affaires; en effet, bien qu'ils soient censés connaitre les règles en vigueur en la matière, ceci n'est pas toujours le cas dans les faits.

Enfin, pour les adjoints de direction, il s'agit là d'un public cible de premier choix, puisque, de par leur fonction, ils ont la possibilité d'avoir accès à des informations sensibles et à haute valeur stratégique (voire confidentielles).

Un élément qui nous semble judicieux de mettre en exergue à ce stade de notre analyse, et qui nous semble relativement écarté par le rapport, est celui des ressources humaines. Comme nous le verrons un peu plus loin, les RH et le help desk sont des portes d'entrées de premier choix pour des pirates ayant monté un bon scénario d'ingénierie sociale. En effet, ce sont là souvent de bons moyens d'attraper

des informations secondaires et/ou primaires[7] pour atteindre ultérieurement les objectifs visés par l'ingénieur social. Ils constituent donc une des premières barrières de défense de l'entreprise. Or, ce type de personnel est souvent écarté et moins bien intégré au processus de formation et de gestion des risques. Si nous nous référons à l'étude, les ressources humaines sont citées à hauteur de 33% comme profil d'employé potentiellement susceptible d'être pris pour cible.

Un constat beaucoup plus inquiétant représenté par la Figure 4 ci-dessous est que seulement 26% des sondés dans leur ensemble, ont indiqué mettre en place des programmes de sensibilisation aux risques incluant la menace d'ingénierie sociale pour leurs employés. Ceci alors que 40% d'entre eux affirment avoir inclus cet élément dans leur politique de sécurité. Notons également que 34% n'avaient rien mis en place au moment de l'étude. Le décalage entre la réalité et les faits est donc non négligeable ; ces trois chiffres à eux seuls nous montrent toutes les possibilités d'amélioration et de sensibilisation qu'il est possible de développer et de mettre en place pour former et sensibiliser à la fois les instances dirigeantes des entreprises et leur personnel. C'est assurément un élément qui doit nous encourager à poursuivre dans cette voie.

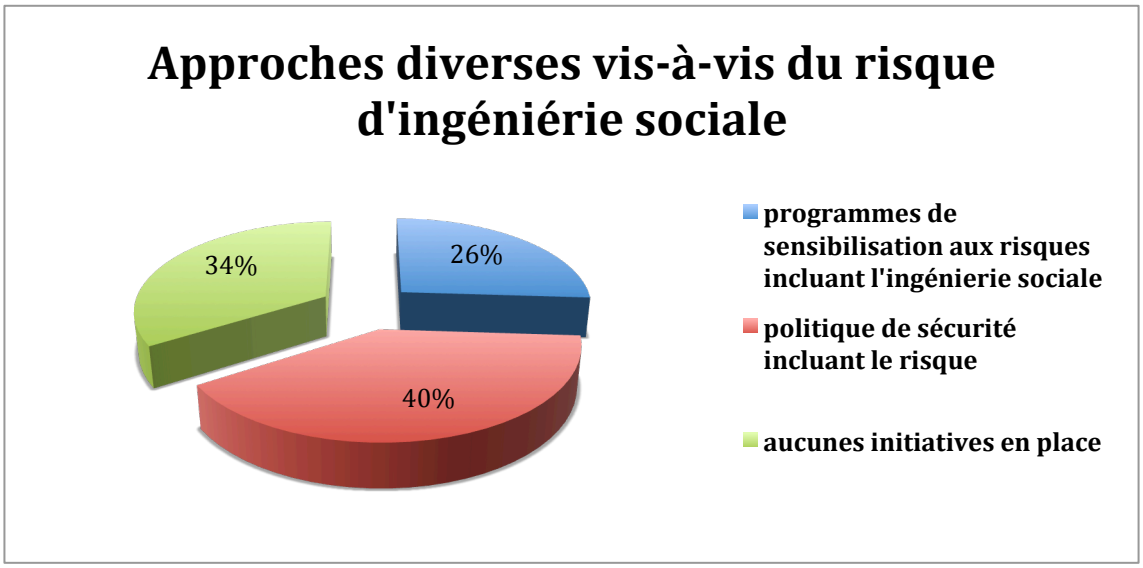


Figure 4 - Approches diverses liées au *social engineering* en entreprise.

7 Par opposition à information primaire (ou stratégique), une information secondaire ne revêt qu'une importance mineure. Il s'agit souvent d'éléments d'informations périphériques (nom d'un employé, fonction, numéro de téléphone etc.) permettant ensuite à l'ingénieur social d'atteindre son but. L'information primaire représente ainsi l'objectif final pour lequel l'ingénieur porte l'attaque. Au contraire, l'information secondaire représente finalement toute pièce d'information qui lui permet d'atteindre son dessein. Cette distinction reste toutefois relative, dans la mesure ou même une donnée qui semble parfaitement anodine peut l'aider dans son processus d'escalade.

Enfin, notons que les deux principaux vecteurs cités par les participants comme étant les moyens les plus usuels pour porter une attaque sont :

- à 47% le *phishing* (cf. glossaire p.85)
- suivi à 39% par les réseaux sociaux

Ces deux points ci-dessus sont d'autant plus intéressants qu'ils ressortent dans la grande majorité des études sur la sécurité informatique en général et des différents articles scientifiques sur le domaine que nous avons pu parcourir[8]. Nous pouvons notamment citer parmi les études consultées celle du CSI[9] : *Computer Crime and Security Survey 2010-2011* et celles du *www.social-engineer.org*[10] : les rapports DEFCON-20, 19 et 18. À l'ère du tout numérique et de l'interconnexion permanente, les sphères privées, sociales et professionnelles des individus sont plus que jamais juxtaposées. Le rôle des nouvelles technologies de l'information et de la communication (TIC) dans ce domaine n'est pas anodin; elles agissent alors comme un catalyseur pour ce type de menace. Ceci fera l'objet d'une analyse ultérieure de notre part dans un chapitre spécialement consacré à cette thématique.

---

8 Voir notamment :

- RAJ, Samani. Re-defining the human factor. *Infosecurity*, 2010, vol. 7, no 2, pp. 30-33
- TOWNSEND, Kevin. The art of Social Engineering. *Infosecurity*, 2010, vol. 7, no 4, pp. 32-35

9 Le *Computer Security Institute* (CSI / www.goCSI.com) est une association professionnelle, basée aux États-Unis (New-York) qui traite de la sécurité de l'information et de la sécurité informatique. Parmi ses nombreuses activités, il publie à raison d'une fois par an un rapport de référence en là matière : *Le Computer Crime and Security Survey.* La dernière version en date que nous avons consulté est celle de l'année 2010-2011.

10 Ce site se veut un cadre de référence dans la discipline de l'ingénierie sociale. Le fondateur de ce dernier, n'est autre que M. HADNAGY Christopher, l'auteur du livre *Social Engineering : The art of Human Hacking*. Il est spécialisé depuis quinze ans dans l'évaluation et la sensibilisation de ce type de risque auprès des entreprises et des responsables de la sécurité. Il propose des stages de sensibilisation, des formations, des tests d'intrusion etc. Depuis maintenant trois ans, il a mis sur pied un test grandeur nature sur ce thème à la conférence annuelle de la sécurité informatique : *Le DEFCON*, qui se tient à Las Vegas. Le but étant de tester en direct les défenses de grandes entreprises de tous secteurs d'activités de l'économie américaine. Les rapports qui s'en suivent (DEFCON-20, 19 et 18) sont des sources d'informations précieuses que nous avons pu consultées.

Le tableau récapitulatif ci-dessous résume les éléments clés que nous avons mis en évidence :

<table>
<tr><th>Prise de conscience</th><th>Survenue de la menace</th><th>Facteurs motivationnels</th></tr>
<tr><td>• 35% en ont conscience
• 62% en ont hautement conscience</td><td>• 45% indiquent que l'entreprise y a déjà fait face
• 41% ne savent pas</td><td>• 51% appât du gain
• 46% accès à des informations stratégiques
• 40% avantages compétitifs
• 14% pour vengeance</td></tr>
<tr><th>Fréquence des attaques</th><th>Cout moyen par incident</th><th>Typologie des employés potentiellement à risque</th></tr>
<tr><td>• 48% des entreprises de 5'000 employés ou plus indiquent 25 attaques ou plus au cours des deux dernières années
• 56% des entreprises toutes tailles confondues indiquent entre 5 et 25 attaques durant la même période</td><td>• 30% des entreprises de 5'000 employés ou plus indiquent un coût moyen de 100'000 dollars US
• 48% des entreprises toutes tailles confondues indiquent un coût moyen par incident de 25'000 dollars US</td><td>• 60% les nouveaux employés
• 44% sous-traitants
• 38% adjoints de direction
• 33% RH</td></tr>
<tr><th>sociale engineering</th><th colspan="2">Principaux vecteurs d'attaque</th></tr>
<tr><td>• 26% du total uniquement</td><td colspan="2">• 47% le phishing
• 39% les réseaux sociaux</td></tr>
</table>

Tableau 1 - Chiffres clés sur l'état de l'art du *social engineering*

En définitive, le bilan semble donc plutôt mitigé. Si un peu plus d'un tiers des professionnels de la sécurité disent en avoir conscience, voire très fortement conscience pour environ deux tiers d'entre eux (cf. p.7), que signifie vraiment cette prise de conscience? Est-ce que cela signifie qu'ils en ont simplement entendu parler? Ou alors ont-ils suivi des séminaires sur ce thème? Mais l'ont-ils pour autant intégré dans la conception de l'architecture sécuritaire de l'entreprise? Alors qu'un peu moins de la moitié d'entre eux affirment que leur entreprise a déjà dû y faire face et que plus de la moitié des sondés indiquent avoir subi entre cinq et vingt-cinq attaques au cours de ces deux dernières années, moins d'un tiers ont mis en place un vrai programme de formation et de sensibilisation. Il y a là un paradoxe qui mérite toute notre attention. Alors que toute une série de risques semblent parfaitement assimilés et connus, celui-ci apparait comme clairement sous-estimé. Une explication possible est de dire que l'ingénierie sociale n'étant pas une technique avancée de hacking (au sens technique du terme), mais plutôt une attaque qui exploite les faiblesses humaines et d'éventuelles failles dans les procédures et/ou processus de l'entreprise; elle est donc relativement intangible. Ainsi, on lui prête moins d'attention qu'à d'autres risques. Pourquoi un pirate perdrait-il son temps et son énergie à devenir un as de l'informatique, alors qu'il est plus facile de s'adresser à celui qui détient les données convoitées?

3. Les quatre étapes d'une attaque d'ingénierie sociale

3.1 Une approche globale

Comme nous l'aborderons plus en détail dans la suite de notre exposé, la sécurité du système d'information de l'entreprise contemporaine n'est plus aujourd'hui la simple affaire des spécialistes de l'informatique. Une approche globale et concertée de la part de l'ensemble des acteurs internes (chefs de département, managers, employés, etc.) et externes (fournisseurs, sous-traitants etc.) est plus que jamais nécessaire :

> *« A team approach to information security, where a large number of people act in a coordinated and directed way, is absolutely necessary if an adequate level of information security is going to be achieved. » (Cresson Wood, 2004, p.17)*

De plus, avec l'arrivée de toute une gamme de nouvelles technologies incluant : les assistants numériques personnels[11] (ou PDA : de l'anglais *Personal Digital Assistant*), le télétravail, l'accès sans fil à distance etc., et le passage à un modèle de distribution de l'information de plus en plus décentralisé (par opposition aux réseaux et ordinateurs de quinze ou vingt ans en arrière ou la structure étant essentiellement celle d'un mainframe centralisant les informations d'une entreprise), les menaces sont de plus en plus complexes, multiformes et mutent de plus en plus rapidement. L'ingénierie sociale mérite à ces égards toute notre attention :

> *« To ensure complete security of an organization from all kinds of internal and external factors, the security consultant must have complete knowledge of the Social Engineering cycle, the techniques that can be used by an attacker and the counter-measures to reduce the likelihood of success of the attack »*[12]

Comme le mentionne cette citation, il est fondamental pour celui qui veut comprendre, mais également intégrer ce risque dans son outil de gestion et d'évaluation des risques, de saisir pleinement quels sont les mécanismes et les étapes de ce type de menace. Une attaque de *social engineering* peut se diviser en deux catégories :

- minimale (ou de courte durée)
- de longue durée[13]

---

11 Un assistant numérique personnel se présente sous la forme d'un appareil numérique portable (appareil dédié, Smartphone etc.) et qui permet entre autre des fonctionnalités comme l'agenda, le carnet d'adresse, le bloc notes etc.

12 Citation tirée du site www.packetstormsecurity.org

13 Les termes : *minimale* et *de longue durée* viennent respectivement de la traduction en français des mots *hunting* et *farming* tirés de l'article :

- RAJ, Samani. Re-defining the human factor. *Infosecurity*, 2010, vol. 7, no 2, p.30

Celle dite *minimale* consiste à extraire (obtenir) les informations souhaitées avec un minimum d'interaction avec la cible, c'est-à-dire tout au plus une rencontre directe. C'est généralement le mode employé pour des attaques éclair au cours desquelles on veut obtenir des informations très rapidement et sans trop se mettre en avant (exemple: le phishing). A l'opposé, celle dite de *longue durée* implique d'établir des rapports plus ancrés, des relations de confiance en vue d'un scénario plus élaboré. L'attaquant sera ainsi amené à rencontrer plusieurs fois sa cible. La différence principale tient donc dans le nombre d'interactions entre les deux parties. En plus de ces deux aspects, une attaque peut être *ciblée* ou *opportuniste*[14]. Dans le premier cas, l'attaquant se concentre sur une cible en particulier (une cible unique et parfaitement identifiée). Dans le deuxième, il cherche à glaner des informations concernant n'importe quel individu occupant une position spécifique (exemple: un membre du Helpdesk).

Une attaque d'ingénierie sociale, se déroule de manière globale en quatre étapes parfaitement distinctes. Chacune d'entre elles fait rentrer en ligne de compte des caractéristiques spécifiques qu'il est important de comprendre pour avoir une compréhension profonde de ce qu'est une incursion de *social engineering*, et en quoi elle se distingue d'une tentative classique de piratage. Toutes ces phases vont demander à l'ingénieur social de faire appels aux quatre éléments d'entrée que nous avons cités dans la Figure 1, p.4 *(*À savoir : *compétences humaines et sociales, habiletés psychologiques, biais cognitifs & compétences techniques)* à des intensités et des rythmes différents. Quant aux éléments de sortie *(*À savoir : *système d'information, information stratégique & bien ou information convoité)*, ceux-ci peuvent déjà prendre place dans la première étape (la récolte d'information), mais surtout dans la troisième partie du cycle (l'extraction)[15]. Notons enfin qu'en fonction du scénario, de la cible et des objectifs du pirate lui-même, la durée de chacune de ces étapes peut varier.

---

14 Les termes : *ciblée* et *opportuniste* viennent respectivement de la traduction en français des mots t*argeted* et *opportunistic* tirés de l'article référencé par la note n°12.

15 Bien que ces aspects peuvent être pris en considération chez le pirate déjà à partir de la première étape du cycle : Quelle est la nature du système d'information? Comment est-il architecturé? Où sont disposées les informations convoitées? Où sont-elles stockées? Etc. Ce n'est véritablement que dans la troisième partie du cycle que la mise en œuvre opérationnelle s'effectue.

La figure ci-dessous visualise ces étapes et leur enchaînement :

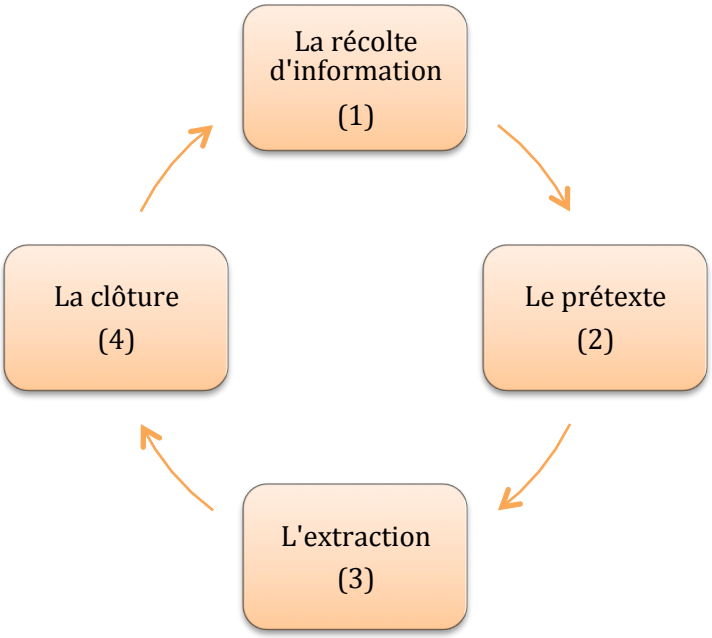


Figure 5 - Les quatre étapes d'une attaque de *social engineering*. Les noms des diverses phases sont tirés de l'anglais. On parle alors de : *Research (ou : gathering Information, footprinting)*, *Hook, Play* et *Exit* pour respectivement la première, la deuxième, la troisième et la quatrième étape ci-dessus. Les chiffres entre parenthèses indiquent l'ordre d'exécution des différentes étapes par le pirate. La boucle complète peut être répétée autant de fois que nécessaire au sein d'une même attaque. Ceci tant que l'attaquant n'a pas obtenu ce qu'il souhaitait, on parle alors de processus d'escalade.

Pour avoir une idée plus claire de comment une attaque peut se matérialiser et afin d'illustrer de manière plus concrète les étapes ci-dessus, nous proposons au lecteur de voir les quelques exemples mis à disposition dans l'annexe suivante : Annexe 1, p.93[16].

3.2 *La récolte d'information*

La phase de récolte d'information est un des points clés pour construire par la suite un prétexte solide, un scénario cohérent et donc une attaque réussie. Elle consiste essentiellement à accumuler suffisamment d'informations sur la (les) cible(s) et leur environnement immédiat, ce qui permettra à l'attaquant d'établir une relation de confiance et d'augmenter ainsi ses chances de réussite au moment de porter l'attaque.

16 Les exemples proposés sont directement tirés du livre suivant :

- MUSSET, Jöelle : *Sécurité Informatique : Ethical Hacking : Apprendre l'attaque pour mieux se défendre*. Editions ENI. France : 2009, pp.68-72

Elle inclut, entre autres, la récolte de données sur :

- Liste des employés avec numéros de téléphones, noms et prénoms, adresses courriels, etc…
- L'organigramme de l'organisation
- La structure de la cible (départements etc.)
- Les fournisseurs
- Site internet corporatif
- Documents publics
- Hobby
- Systèmes de sécurité et plans d'entreprise
- Type de logiciels, de hardware avec les versions
- Topographie du site
- Politiques de l'entreprise
- Processus métiers et activités commerciales
- Projets en cours
- Etc.

La liste ci-dessus n'est de loin pas exhaustive. De plus, les éléments d'information dont le pirate aura besoin vont fortement dépendre du contexte dans lequel se déroule l'attaque, du (des) but(s) visé(s), etc. Afin de réaliser cette cueillette, il peut alors faire appel à toute une série d'outils dont les principaux sont essentiellement : les réseaux sociaux, les moteurs de recherche, les sites Web d'entreprise et autres blogs, des outils de recherche et de collecte de données (exemple : Maltego[17]), des services d'annuaire du Web (exemple : Whois[18]) et bien sûr l'accès physique au site. Cette dernière méthode, bien que plus risquée, peut présenter un certains nombres d'avantages pour un attaquant expérimenté. Elle peut lui permettre d'évaluer si son scénario est suffisamment viable (mûr) pour être lancé, si des compléments d'information peuvent s'avérer utiles ou encore repérer d'éventuelles failles subséquentes auxquelles il n'avait peut-être pas prêté attention initialement. Ainsi la récolte d'information comprend deux sous-parties :

---

17 Ce logiciel open-source, permet de récolter et modéliser les relations entre différentes données sur une organisation ou une personne. Par le biais de graphique, il est alors possible de déduire de nouvelles liaisons (informations) et/ou effectuer du forage de données.

18 Ce terme est une contraction de l'expression anglaise *who is?*, qui signifie *qui est-ce?,* en français. Il s'agit d'un service de recherche Web fournis par les registres internet. Il permet d'obtenir des informations sur une adresse IP ou un nom de domaine quelconque : http://www.whois.net

La recherche passive :

Elle consiste à glaner toutes les informations jugées utiles sur la cible, mais sans rentrer en contact direct avec elle. C'est-à-dire sans se rendre sur site directement. C'est là que les réseaux sociaux, les moteurs de recherche et autres objets de ce type interviennent pour aider le pirate dans son œuvre.

La recherche active :

Il s'agit d'affiner, de compléter ses informations sur la cible et son environnement avec la possibilité de rentrer en contact direct ou indirect (p.ex. : courriel(s), appel(s) téléphonique(s), scanner les ports pour avoir une topologie du réseau etc..), visiter physiquement le site d'entreprise (caméra(s), systèmes de sécurité etc.).

Cette première étape peut être plus ou moins longue et dans certaines circonstances elle peut même s'avérée optionnelle. En effet, suivant le type d'attaque mis en œuvre (p.ex. : le phishing, les périphériques malicieux[19] etc.) il n'est pas nécessaire pour le pirate de mener une telle recherche d'informations. Elle est d'ordinaire plutôt employée lorsque l'attaque est complexe et qu'il s'agit de s'intéresser à une ou deux personnes clés de l'organisation pour arriver à ses fins.

L'attaquant peut alors déterminer plus finement qu'elle est la meilleure personne à approcher et le(s) meilleurs(s) moyen(s) de l'engager (points faibles, pressions, point de leviers).

3.3 Le prétexte

Une fois la reconnaissance effectuée, il s'agit pour l'attaquant, sur la base des informations précédemment acquises, de construire un prétexte (et un scénario) fiable et viable vis-à-vis de sa victime. Les liens de confiance que celui-ci va réussir à tisser à ce stade avec sa proie lui seront utiles dans la phase suivante pour se procurer les informations stratégiques qui lui permettront de mener son scénario à terme. C'est ici que les compétences humaines et sociales, ainsi que les habiletés psychologiques du pirate vont prendre tout leur sens. Enfin, l'utilisation des biais cognitifs va lui permettre

19 Ce terme se réfère généralement à tout support digital et/ou mécanique qui est externe à un ordinateur (exemples : clé USB, CD-ROM, DVD-ROM, souris etc.). Comme nous le verrons dans le chapitre suivant, ce sont d'excellents vecteurs pour tout ingénieur social voulant introduire malicieusement des logiciels malveillants au sein du système d'information de la cible.

de prendre le contrôle de l'échange sur sa cible en renforçant son influence et son pouvoir de persuasion.

3.3.1 Les biais cognitifs

Un biais cognitif peut être défini comme suit :

> *« Un biais cognitif est une erreur dans la prise de décision et/ou le comportement adopté face à une situation donnée résultant d'une faille ou d'une faiblesse dans le traitement des informations disponibles.» (Jacquet, 2010, p.25)*

Nous pouvons alors distinguer les principales faiblesses psychologiques suivantes sur lesquelles l'ingénieur social va s'appuyer pour son attaque :

1. ***La réciprocité***[20]
   a. **Description**

      Manipuler quelqu'un pour qu'il se sente reconnaissant et obligé vis-à-vis de l'ingénieur social. Il en résulte souvent un ressenti de la victime qu'il doit une faveur à l'ingénieur social.

   b. **Illustration**

      Après avoir finement préparé son scénario, le pirate se présente au siège la société *Software S.A.*, spécialisée dans le développement de produits logiciels bancaires. À son arrivée, il se présente auprès de la réceptionniste et constate que celle-ci est en train de se débattre avec son imprimante : « zut et re-zut !! Cette satanée machine ne fonctionne pas et le rapport devrait déjà être sous pli (dit-elle) ». C'est alors tout naturellement qu'il lui propose son aide car : « j'ai travaillé pour ce fabricant pendant cinq ans (prétexte-t-il) ». La secrétaire paniquée, accepte volontiers son assistance. Se sentant obligée : « Merci beaucoup, vous m'avez été d'un grand secours. Que puis-je pour vous?». La brèche étant ouverte, le pirate peut s'y engouffrer :

      Attaquant : « J'ai rendez-vous cette fin de semaine avec votre responsable des RH, Mr. MOORE je crois, et je dois lui confirmer ma

[20] Ce biais est important car il crée automatiquement chez la victime un sentiment d'obligeance inconscient. Elle se retrouve donc dans une position de faiblesse psychologique, qui l'amène à être enclin à coopérer et divulguer plus facilement des informations. Plus de détails avec des exemples pratiques peuvent être consultés dans l'ouvrage suivant :

- HADNAGY, Christopher. *Social Engineering : The Art of Human Hacking*. Wiley Publishing, Inc. Indianapolis, Indiana : 2011. pp.188-195

venue. Toutefois, j'ai égaré sa carte de visite avec ses coordonnées. Vous seriez bien aimable de me les redonner ».

Secrétaire : « Avec grand plaisir, et voici à vous toutes les informations nécessaires ».

Prenant ainsi congé de cette dernière, le pirate a obtenu les informations escomptées et pourra mener son processus d'escalade ultérieurement.

2. *L'envie d'être utile (d'aider autrui)*

a. Description

Dans leur désir d'être utile et de résoudre les demandes d'autres usagers, les personnes ont tendance à donner beaucoup d'informations qui ne doivent pas être nécessairement divulguées à l'extérieur. Celles-ci pourraient donner à un attaquant une chance d'obtenir un accès non autorisé au système cible causant une perte possible d'information.

b. Illustration

L'attaquant se fait passer pour un client (ou client potentiel) quelconque et appelle le service client d'une célèbre marque de Smartphones. Après une brève première prise de contact, il prétexte le souhait de faire l'achat d'un nouveau matériel, mais n'est pas sûr de la compatibilité du produit avec son installation à domicile.

Il commence alors par questionner l'opérateur sur la version de l'OS[21] à employer. Il en profite également pour demander quel navigateur l'opérateur lui conseillerait, quelle version est présente sur les machines actuelles à l'achat, quel est le client mail par défaut et sa version etc. Autant de questions relativement ennuyeuse et anodines qui lui permettent de soutirer de l'information.

Il peut également jouer la comédie en deux temps, en prétextant le besoin d'un temps de réflexion pour son achat définitif. Il lui demande alors s'il est possible de rappeler plus tard, quelles sont les heures d'ouvertures et quel est son nom, son numéro de ligne directe car il a

21 De l'anglais *Operating system* (en français : Système d'exploitation), ce terme se réfère à l'ensemble des logiciels qui permettent la gestion du fonctionnement de nos ordinateurs, tablettes, Smartphone etc. Nous pouvons citer entre autre: Windows, Mac OS, Linux etc.

été très bien servi par lui (flatte un peu) et aimerait de nouveau avoir affaire avec ce dernier. Il y a fort à parier que tout ceci fonctionne sans peine puisque les services clients en général sont justement formés pour être aidants, accueillants et chaleureux. Dans une économie de marché comme la nôtre, de nombreuses compagnies veulent faire plaisir et gagner de nouveaux prospects. Il est alors tout naturel de répondre à leurs demandes.

3. *La rareté (La crainte de perdre quelque chose)*

a. Description

Manipuler la victime en menaçant l'approvisionnement à court terme de quelque chose dont elle a besoin (ou qu'elle veut).

b. Illustration

Dans les grandes entreprises, il n'est pas rare que tout ou partie du service informatique soit outsourcé[22] (ou éventuellement situé dans un bâtiment différent de celui ou se prennent les décisions stratégiques, opérationnelles etc.) De ce fait, les équipes ne se connaissent pas toujours. Marc le sait bien et s'est déjà renseigné en ce qui concerne la société de développement de jeux vidéo : *Games S.A.* Il décide alors de porter une première attaque et appelle la réceptionniste du groupe :

Réceptionniste : « *Games S.A.* bonjour. Justine pour vous aider, que puis-je pour vous? »

Marc : « Bonjour Justine. Ici Julien du service informatique à Genève. Comment allez-vous? »

Réceptionniste : « Très bien, merci et vous? »

Marc : « Pour des raisons de maintenance urgente, nous allons devoir interrompre l'accès à un certains nombres de services dans le courant de l'après-midi. J'appelle pour dresser une liste des gens à rétablir rapidement. Pourriez-vous travailler sans le téléphone et internet pendant cette demi-journée? »

Réceptionniste : « (Angoissée et déstabilisée), j'ai beaucoup de travail cette après-midi, des appels à effectuer, des réservations etc., cela me

22 Cf. glossaire p.81

semble compliqué. Ne serait-il pas possible de faire ceci plutôt en fin de semaine? »

Marc : « Malheureusement non, pour des raisons de sécurité, nous devons agir rapidement »

Réceptionniste : « Bon très bien. Comment faire pour que ça aille au plus vite?»

Marc : « J'ai uniquement besoin pour cela de deux ou trois informations de votre part : le numéro de votre poste, votre nom d'utilisateur et mot de passe, s'il-vous-plaît. »

Réceptionniste : « Pas de problème pour les deux premières informations. Mais j'ai reçu il y a peu une note qui m'indique de jamais divulguer mon mot de passe, même au service informatique. Avez-vous changé d'avis? »

Marc : « Non, les autres employés vont devoir le remettre eux-mêmes car nous rétablissons les services département par département, mais cela risque de prendre plusieurs heures. Pour aller plus vite, je vais rentrer le vôtre directement. Ainsi, vous pourrez reprendre votre travail dès le retour de votre pause déjeuner. »

Réceptionniste : « Ah d'accord. Alors mon mot de passe est *password123*. »

Le fait de créer un sentiment d'urgence dans l'esprit de l'usager, couplé avec la menace en approvisionnement d'une ressource (matériel, alimentaire etc.) peut créer une faille de sécurité. Le pirate pourra ainsi tenter une escalade par privilège.

4. *Le respect de la parole donnée) & la cohérence (la consistance)* [23]

a. Description

- *Respect de la parole :*

  La nature humaine est ainsi faite que les gens essaient généralement de s'en tenir à leurs promesses et de tenir leur parole, afin de ne pas paraître douteux, suspect ou de peu de confiance.

- *La cohérence (la consistance) :*

  Les personnes essayent généralement d'être cohérentes (consistantes) dans leurs propos et comportement. De la même façon, ils attendent la même chose de la part d'autrui.

Ces sentiments sont souvent basés sur les intuitions personnelles et les expériences passées de l'individu. Je me suis engagé à, j'ai fait l'expérience de telle ou telle situation etc. Donc on attend de moi, tel comportement, telle réponse (cohérence - consistance). Voilà pourquoi ces dimensions sont très fortement interreliées.

b. Illustration

Pierre est un ingénieur social averti. Il s'est donc déjà renseigné sur la société qu'il a décidé d'attaquer, et ça sera *3Tech Sarl.* Il dispose notamment des informations sur l'architecture de son réseau, ainsi que sur la compagnie de support technique (informatique) à laquelle cette dernière fait appel pour la gestion de ses serveurs. La société à responsabilité limitée est active dans le e-Commerce, et possède plusieurs salles serveurs en son sein avec des données clients sensibles.

Dans le cadre de ses activités d'espionnage industriel, le pirate a été mandaté par une société concurrente afin de soutirer des informations sur les clients importants de chez *3Tech Sarl.* En effet, son client est à la traîne sur certains marchés et il aimerait appâter certains des prospects de son concurrent pour gagner des parts de marché.

---

[23] Le nom de ce biais provient de la traduction des mots anglais suivants : *commitment* et *consistency*. Pour plus de détails :

- HADNAGY, Christopher. *Social Engineering : The Art of Human Hacking*. Wiley Publishing, Inc. Indianapolis, Indiana : 2011. pp.202-206

Il se présente alors à la réception de *3Tech Sarl* avec toute la panoplie du parfait technicien informatique. Tout naturellement, il demande l'accès à la salle serveur principale. Cela tombe bien (car comme par hasard), il y a de la congestion sur le réseau lui indique gentiment l'assistante. La demande qu'il effectue étant cohérente et consistante avec les expériences et les attentes vécues par le passé, l'assistante oublie de faire les vérifications d'usage. Pierre accède alors à la salle voulue avec toutes les possibilités que cela lui ouvre.

Voilà comment une action anodine de la part d'un collaborateur peut créer involontairement une brèche de sécurité.

5. *La sympathie (l'affection)*

a. Description

Les gens sont plus susceptibles de se conformer aux demandes de quelqu'un qu'ils aiment, qu'ils apprécient ou qu'ils connaissent.

b. Illustration

Pour cette illustration, nous citons directement un extrait tiré d'un document de recherche que nous avons pu nous procurer au cours de nos travaux[24]:

« The caller presented himself as a member of the IT services. He mentioned several colleagues and supervisors in an appropriate position. He also incorporated some of the researched additional information, such as the "conincidence" of having studied at the same university. This information was interwoven in the phone call and only mentioned in passing, but eagerly taken up by the administrator.
At the end of the call, the first person was very close to providing the password, but did not want to do so over a phone line. The second phone call to another. administrator was successful. »

Un autre papier de recherche montre également l'impact que peut avoir la force du lien social qui unit deux personnes, dans le succès ou non d'une attaque[25] :

- 33% de chance de réussite si se sont de parfaits étrangers,

---

24 L'extrait cité est directement tiré du document suivant :

- Rössling, Guido et Müller, Marius : *Social Engineering : a serious underestimated problem,* Proceedings. p. 384

25 Les chiffres sont directement tirés de l'article suivant :

- FURNELL, Steven, ZEKRI Leith. Replacing passwords : in search of the secret remedy. *Network security*, 2006, vol. 2006, no 1, p.6

- 38% si se sont de simples collègues,
- 66% s'il existe un lien d'amitié
- 87% s'il y a un lien de parenté.

L'ingénieur social à donc tout intérêt à se montrer à l'écoute de ses victimes et tisser un lien privilégié avec elles.

6. La figure d'autorité (la peur de l'autorité)

a. Description

Les gens se conforment à la demande lorsque la requête provient d'une figure d'autorité[26]. En effet, beaucoup d'individus sont inquiets de la présence d'une personne qu'ils perçoivent comme une figure d'autorité. L'inquiétude ne provenant pas de la personne elle-même, mais de la position et du pouvoir de la personne qui les intimide.

b. Illustration

Dans le cadre d'un audit de sécurité, le consultant peut usurper l'identité du CEO ou de tout autre personne qui occupe un poste hiérarchique dans une position de pouvoir au sein de l'entreprise. Ainsi, il peut par exemple tenter d'obtenir des mots de passe auprès du help desk, ou de soutirer d'éventuelles informations sensibles auprès de n'importe quel autre collaborateur le percevant comme une figure d'autorité. Avec les bons vêtements, le bon langage corporel et pourquoi pas une fausse carte de visite, il y a de très forte chance que ceci fonctionne. C'est d'ailleurs un stratagème souvent employé par les ingénieurs sociaux pour gagner l'accès à un bâtiment ou voler des informations précieuses.

7. La validation sociale

a. Description

Les personnes respectent et accèdent plus facilement aux demandes quand les autres font la même chose. Ce biais intervient :

- Dans les situations d'ambiguïtés et d'incertitudes. Nous observons et reproduisons le comportement social d'autrui.
- S'il y a une identification forte avec les valeurs et le statut de la personne.

---

26 On distingue généralement trois formes d'autorité : *l'autorité légale* (policiers, avocats administrations d'état etc.), *l'autorité hiérarchique* (typiquement un supérieur hiérarchique qui occupe un poste de pouvoir : CEO, CIO etc.) et *les leaders naturels*.

b. Illustration

Reprenons notre exemple ci-dessus, du consultant menant son audit de sécurité pour une grande entreprise à l'international. Ce dernier pourrait se présenter tout bonnement à l'entrée principale du bâtiment, et dire au vigile responsable de la sécurité physique quelque chose du type : « Hier, Jim m'a laissé entrer après avoir vérifié toutes mes accréditations. Je pensais que tout était en ordre.» Une phrase aussi anodine que celle-ci, doublée d'un vigile un peu endormi par ses tâches répétitives peu suffire à gagner un accès non autorisé.

8. L'excitation de la victoire (d'avoir gagné quelque chose)

a. Description

L'excitation liée à un gain[27] (généralement fictif) suscite de la joie et du bonheur chez l'individu. En se laissant emporter par ses sentiments, il est facile de perdre la raison et d'oublier les règles de base. L'attaquant peut ainsi profiter de cet état de liesse pour obtenir ce qu'il veut de sa victime.

b. Illustration

Claire, assistante de direction un peu crédule, reçoit un courriel pendant qu'elle travaille au bureau. En voici son contenu :

« Chère Madame, après un premier tirage au sort effectué par nos soins, nous sommes heureux de vous annoncer que vous avez été présélectionnée pour la cagnotte finale de 100'00 euros. Afin de participer au tirage final et avoir la chance de remporter la somme du gagnant, nous vous demandons de remplir votre formulaire de participation en cliquant sur le lien ci-dessous:

www.jeveuxgagnerdessous.com

En espérant vous compter prochaines parmi nos heureux gagnants, nous vous adressons, Madame, nos meilleures salutations.

L'équipe de la française des jeux. »

---

27 Dans certains cas, bien peu de chose suffisent pour résussir à soutirer des informations sensibles comme par exemple des mots de passe. Avec la simple promesse de gagner un stylo ou une barre de chocolat, il est possible d'arriver à ses fins:

- FURNELL, Steven, ZEKRI Leith. Replacing passwords : in search of the secret remedy. *Network security*, 2006, vol. 2006, no 1, p.4

Toute contente face à cette situation inattendue, Claire se dit que c'est là une occasion en or qu'il faut saisir. Elle se plait déjà à imaginer ce qu'elle pourra faire de cet argent. Ainsi, elle décide de cliquer sur le lien car au fond, c'est peut-être la chance de sa vie. Le mal est fait puisque ce dernier lance à son insu le téléchargement et l'installation en toile de fond d'un logiciel malveillant (exemple : un keylogger[28]). Le pirate prend ainsi le contrôle à distance de sa machine et de ses données.

9. La paresse (la lassitude)

a. Description

Chaque personne a une partie ou l'autre de son travail quotidien qui exige d'elle de ne faire qu'un ensemble spécifique et répétitif d'activités. Ceci engendre des situations d'ennui intellectuel chez la personne qui effectue les mêmes tâches à plusieurs reprises sur une base quotidienne. Elle apprend à développer des raccourcis pour exécuter les tâches en utilisant un minimum d'efforts et en respectant les objectifs. De tels individus, sont plus susceptibles de devenir paresseux et sont plus sensibles à des attaquants. En effet, en raison de l'attitude décontractée de ces personnes vis-à-vis de leur travail, il est plus aisé de leur subtiliser de l'information.

b. Illustration

Si nous imaginons certains postes un peu rébarbatifs comme celui de notre vigile précédent ou notre assistante de direction crédule, il est alors aisé de comprendre les conséquences que cela peut avoir pour la sécurité.

Dans le cas du vigile qui reste assis toute la journée à contrôler des badges d'entrée, il est facile de se laisser aller ou de prendre des raccourcis dans une tâche qui se veut ennuyeuse, simpliste et ne lui apportant que peu intellectuellement. Ainsi, en s'appuyant (en combinant) sur un autre biais (exemple : la figure d'autorité), il est possible de lui subtiliser de l'information.

De la même manière pour l'assistante dont l'essentiel des tâches sont très certainement réglées comme du papier à musique, nous pourrions

28 Cf. glossaire p.81

combiner celui-ci avec *l'ego*. En la flattant, en s'intéressant à elle et en créant un lien privilégié, l'ingénieur social arrivera sans trop de peine à ses fins.

10. L'ego

a. Description

L'attaquant rend la victime plus émotionnellement sûre d'elle en se montrant à son écoute et en (sur)valorisant ses compétences. En flattant ainsi son ego, l'ingénieur social supprime la prise de conscience logique dans l'esprit de la victime.

b. Illustration

Il s'agit ici pour l'attaquant de s'intéresser sincèrement à la personne cible : ce qu'elle est, ce qu'elle fait, ses envies, ses passions, ses croyances, ses goûts etc. Les compliments (renforçateurs positifs), l'apparence (c'est-à-dire le look général) et le cadre (l'atmosphère) que celui-ci véhicule sont autant d'éléments importants dans sa mise en scène.

On peut parfaitement imaginer un scénario ou le pirate engage la conversation avec sa victime par l'emploi d'une phrase aussi banale que : « Ce sont de jolies chaussures que vous avez là ; où les avez-vous acheté? » En effet, les individus aiment et apprécient le renforcement positif. Et ce tout particulièrement lorsque celui-ci est dirigé vers eux. En recevant un compliment d'autrui, la personne va avoir envie de rester au contact et probablement de s'ouvrir plus. Par ailleurs, l'ingénieur social peut renforcer cet effet, en alimentant la discussion avec d'autres questions entremêlées de renforçateurs positifs. La cible se sent alors d'une certaine façon unique, spéciale.
Un peu comme si le pirate avait une haute compréhension de ce qu'elle est, de ce qu'elle pense etc. Petit à petit, ce lien qu'il aura tissé lui donnera la possibilité de mettre la personne en très grande confiance et d'obtenir frauduleusement ce qu'il convoite.

11. Le manque de connaissance (l'ignorance)

a. Description

Les connaissances sur le système cible sont un des facteurs clés qui différencient l'attaquant des autres employés de l'organisation. À cause

du manque de formation adéquate, les employés eux-mêmes ne savent pas s'ils ont des connaissances complètes sur les produits, les processus de l'entreprise etc. Les ingénieurs sociaux profitent de telles situations, en créant un sentiment d'urgence et de stress psychologique ne permettant pas à l'employé de prendre le temps nécessaire à l'analyse et la décision. Ainsi, ils ne perçoivent pas le fait qu'ils sont l'objet d'attaques.

b. Illustration

Justin est un chasseur de têtes peu scrupuleux. En cette fin d'année, il aimerait réussir à recruter un ingénieur au profil très particulier pour l'un de ses clients important. Ainsi, il espère doubler sa prime. C'est alors qu'il décide de décrocher son téléphone et d'appeler la société concurrente *ITSystems Sarl.* S'engage alors la conversation :

Standard : « Société *ITSystems,* bonjour, que puis-je pour vous? »

Justin : « Bonjour. Je vous appelle car c'est urgent, nous avons un problème avec l'un de vos produits, le *TEC-402.* J'aurai aimé rapidement joindre l'un de vos techniciens pour de l'aide si c'est possible, merci. »

Standard : « Oui, bien entendu, je vous mets en relation avec notre service après-vente. Un instant svp. »

Justin : « (La voix un peu pressé), Voyez-vous, il s'agit d'un problème de compatibilité entre le logiciel de votre produit et certains de nos équipements ici. Votre produit fonctionne bien, toutefois, j'aurai aimé discuter avec un expert pour savoir si une solution est possible, et si les appareils peuvent cohabiter ensemble. »

Standard : « Pas de problème. Je vous mets directement en relation avec notre ingénieur responsable. Bonne journée. »

Justin : « Merci, au revoir. »

La personne à la réception n'a probablement pas connaissance du produit. Et plus grave encore, elle ignore que joindre directement un des experts peut s'avérer dangereux.

La liste des biais que nous avons présenté ci-dessus, n'est pas exhaustive, mais met en lumière les principaux points de leviers dont dispose l'ingénieur social (deux autres

exemples sont données ici : Annexe 2, p.96). Les différents éléments ne sont pas forcément toujours valables (pertinents) car tout va dépendre du contexte de l'attaque, des informations recueillies par avance (reconnaissance) et celles glanées sur le moment ainsi que du scénario que le malfaiteur aura choisi et mis en place. De plus, comme nous l'avons laissé entrevoir dans nos diverses illustrations, ces deniers peuvent être combinés entre eux suivant les circonstances. Un scénario et donc l'attaque en elle-même, n'est pas quelque chose de figé, de statique. Le pirate doit être capable de combiner, modifier, ajouter ou supprimer un élément à sa guise pour amplifier, ajuster la portée de ses actes et arriver à ses fins. Tout ceci, mis en relation avec les techniques d'ingénierie sociale que nous verrons plus en détails dans les prochaines pages de notre recherche, constitue la boîte à outil de notre pirate.

Notons aussi que ces techniques, ne sont pas spécifiques au domaine du *social engineering,* mais ce sont plutôt des constituantes de la psychologie, du « hardware humain » qui peuvent être exploitées dans toute une série de contextes. Notre centre d'intérêt est ici la sécurité du système d'information, mais vous pourriez imaginer des applications au domaine politique, pharmaceutique, dans le marketing etc.

On ne peut pas sérieusement exhaustivement retenir tous les biais pour les inculquer à ses employés et espérer ainsi ne plus se faire avoir. Ni tomber dans la paranoïa la plus totale et ne plus oser bouger ou dire quoi que ce soit. Toutefois, il est absolument fondamental d'en avoir conscience. Une entreprise doit, sur la base de ses besoins, ses expériences passées, sa vision stratégique etc. être capable de sensibiliser, former et rendre attentif son personnel à ces éléments. Tout du moins à ceux qui s'avèrent pertinents pour elle. Mieux le personnel saura reconnaître et visualiser les signes avant-coureurs d'une telle menace, plus la sécurité globale de l'entreprise en sera améliorée:

> *« A well-trained and educated human is worth far more than any automated system in terms of actual defense. »*[29]

Nous comprenons aussi mieux pourquoi à la vue de ces éléments, ce risque représente une si grande menace. Il repose en effet sur des failles humaines intangibles auxquelles aucun système cryptographique, aucune mise à jour, aucun

---

29 La citation est tirée du rapport : *Social Engineering Capture the Flags Results – Defcon 19* écrit par *M. HADNAGY Christopher.* Le document peut être consulté à l'adresse suivante : http://www.social-engineer.org, via l'onglet CTF du menu principal en haut de la page d'accueil.

patch de sécurité ne peut remédier. La formation régulière, adaptée et répétée du personnel constitue alors l'une des meilleures contre-mesures possibles.

Toute ceci à pour but de créer un lien qui semble légitime et sincère aux yeux de la victime pour établir avec force son scénario et extraire dans la phase suivant les données et/ou biens souhaitées. Au final les points importants qui constituent l'étape du prétexte sont au nombre de quatre :

1. Engager la victime
2. Raconter l'histoire et mettre en place le prétexte
3. Construire une relation de confiance
4. Prendre le contrôle de l'échange

3.4 L'extraction

Dans cette étape, il s'agit d'user du prétexte et de la confiance mis en place précédemment pour extraire les données stratégiques et causer les dommages à l'organisation. Le pirate tire profit de tout ce qu'il a préparé auparavant pour atteindre son (ses) but(s) et faire en sorte que l'attaque soit une réussite pour lui. Ceci peut durer autant que nécessaire mais nécessite les éléments clés suivants :

1. Maintenir le scénario (l'histoire) crédible en l'alimentant sans cesse avec des éléments nouveaux et pertinents au fur et à mesure que la relation avance
2. Garder un contrôle constant et rapproché avec la cible
3. Récolter les informations sans éveiller de potentiels soupçons

À ce stade, il peut en fonction de son analyse personnelle, de l'environnement dans lequel il se trouve, de la disposition et/ou la présence de certains acteurs ainsi que des opportunités du moment :

- Soit passer à la prochaine cible et rentrer dans un processus d'escalade (imaginons une attaque en plusieurs étapes, plusieurs niveaux : on commence par l'assistant pour ensuite cibler la responsable RH)
- Ou garder sous son contrôle sa première victime, continuer à alimenter son histoire en répétant le cycle si nécessaire pour soutirer tout ce dont il a besoin.

Dans tous les cas, il doit également penser à planifier sa sortie éventuelle en imaginant un prétexte plausible et une façon de cacher ses traces une fois son action complétée, notamment pour ne pas paraitre suspect aux yeux de sa (ses) cible(s). Une autre alternative possible serait, dans le cas où la cible à une haute valeur stratégique à ses yeux, de partir tout en conservant un accès aussi privilégié que discret au système

d'information de l'entreprise via une porte dérobée[30]. Il pourra ainsi revenir à sa guise le moment venu.

3.5 La clôture

Au final, après avoir obtenu ce qu'il voulait, l'ingénieur social doit effectuer une sortie propre pour éviter d'attirer une quelconque suspicion sur sa personne. Ceci doit être réfléchi et pensé bien avant de rentrer dans le jeu. Il doit notamment s'assurer de ne laisser paraitre aucune information susceptible de remonter à sa réelle identité ou pouvant le relier à ses méfaits. Cependant, dans certaines circonstances bien particulières, il est possible pour lui de ne pas prêter grande attention à ces bonnes pratiques en matière d'exfiltration :

- Soit parce que l'entreprise n'a pas (ou peu) de système de traçabilité des incidents. Ce qui lui permet d'agir en toute sérénité.
- Soit parce qu'il opère depuis l'étranger et ne tombe pas sous le coup d'une loi dans la zone géographique où est présente sa cible (typiquement dans certaines attaques à distance pour de l'espionnage industriel)

30 Cf. glossaire p.81

4. Techniques et outils pour l'ingénierie sociale

4.1 Les réseaux sociaux et le Web en général

L'avènement du *Web 2.0*[31] (ou *Web participatif*) et le développement fulgurant des outils et technologies associées ont conduit à une plus grande démocratisation des nouvelles technologies de l'information et de la communication. Parallèlement à cela, l'expansion croissante de l'informatique domestique (ou informatique tout public) avec les ordinateurs portables, les tablettes numériques et autres Smartphones ont considérablement accélérés l'entrecroisement des sphères privées, sociales et professionnelles. Nous sommes maintenant connectés quasiment partout et tout le temps. Si bien que les frontières qui autrefois déterminaient clairement le contour de chacune de ces sphères sont aujourd'hui beaucoup plus floues. Le privé se mélange au professionnel, le professionnel s'invite dans le privé, etc.

Aujourd'hui, même en entreprise des outils comme *Facebook*, *Google+, LinkedIn*, *Twitter* et autre *Xing* sont devenus des outils à forte valeur ajoutée et de plus en plus fréquemment employés. Deux études menées par le groupe *Forrester*[32], résument parfaitement à elles seules la portée de ces nouveaux outils sur le plan de l'économie d'entreprise :

- En 2009, 18% des entreprises sondées ont indiqué déjà avoir recours (12%) ou avait planifié l'utilisation des médias sociaux (6%) pour leurs activités au cours de l'année 2010.
- En 2010, 49% des entreprises sondées ont indiqué vouloir augmenter leurs investissements dans ces technologies pour l'année 2011.
- Et 32% d'entre elles avaient déjà indiqué l'emploi d'une forme ou d'une autre de média social pour l'année 2010.

Dans une économie de marché quasi saturée ou il s'agit de gagner de nouvelles parts de marché, de fidéliser et attirer de nouveaux prospects, de renforcer la position de sa marque, d'augmenter sa visibilité et si possible tout ceci plus vite que la concurrence,

---

31 On parle généralement du *Web 2.0* comme un *Web participatif* puisque le développement des nouvelles technologies qui lui sont associées permettent tout à chacun de nos jours de créer son propre site, son blog, de prendre position sur un forum etc. Ceci par opposition généralement au *Web 1.0* qui était l'affaire de spécialistes du domaine. En effet, il n'y a si longtemps, l'édition d'une simple page HTML demandait des compétences informatiques dans le domaine.

32 Les données sont tirées des deux études suivantes :

- CHENXI, Wang. Your Anti-Social Behavior Stops Here – Set Guidelines To Adopt Social Media And Reduce Risk. p.2
- CHENXI, Wang. To Facebook Or Not To Facebook – A social Computing Report. p.2

ces nouveaux outils sont alors perçus comme un nouvel eldorado pour le département marketing et ventes des plus grandes entreprises. On ne compte plus le nombre d'entreprises qui ont leur site Web, leur page Facebook ou encore leur compte Twitter. Ces nouveaux outils élargissent considérablement le champ du possible, en permettant notamment de connaître quasiment instantanément les goûts des consommateurs, par exemple en les faisant voter sur le lancement d'un nouveau produit, en leur permettant de donner leur opinion et/ou de prendre part au lancement d'une nouvelle pub, une nouvelle marque, de sponsoriser une activité[33], de réagir directement à leurs prises de position[34], d'atteindre des clients qui jusque-là restaient hors de portée ou encore en s'évitant de coûteuses et fastidieuses études de marchés. Si nous ajoutons à cela, les blogs spécialisés et le développement du Wifi gratuit (ou presque) un peu partout, nous aboutissons finalement à un joyeux *melting-pot* dans lequel, les différents agents économiques sont quasi en permanence connectés les uns avec les autres.

De façon un peu plus formelle, le développement d'outils comme le télétravail, la possibilité d'accéder à distance à son bureau ou encore des mouvements comme le *Bring Your Own Device*[35] permettent également une plus grande souplesse dans nos activités professionnelles quotidiennes. Toutefois, ce qui fait le bonheur des uns, fait le malheur des autres. Avec toutes ces nouvelles technologies, l'information (au sens large du terme) qui était autrefois centralisée et essentiellement géré par des spécialistes se retrouve aujourd'hui disséminée un peu partout. Que ce soit pour les besoins du personnel de l'entreprise qui travaille à distance ou se trouve en déplacement, en passant par ceux des sous-traitants, des partenaires commerciaux etc. chacun revendique son droit d'accès au système d'information de l'entreprise. Tout ceci n'est pas sans conséquences sur la gestion des risques (et plus particulièrement celui qui nous intéresse) et pose des défis majeurs aux gestionnaires.

---

33 À cet égard, *la production participative* (ou *crowdfunding* : en anglais) constitue un exemple tout à fait intéressant. Un très grand nombre de personnes décident de mettre en commun des fonds pour la production participative d'un projet de création. Pour en savoir plus : http://en.wikipedia.org/wiki/Crowdfunding

34 Un bon exemple de ceci est celui des CFF, qui au début de cette année avaient alloué un staff complet de collaborateurs pour répondre aux diverses missives des clients lors du changement d'horaire sur le réseau.

35 Le *Bring Your Own Device* (ou abrégé *BYOD* en anglais), c'est-à-dire : *Apportez vos propres appareils* (ou plus formellement *PAP* pour : *Prenez vos appareils personnels*), est un mouvement dans l'air du temps, qui incite le personnel à prendre ses propres appareils (PC etc.) sur le lieu de travail pour effectuer leurs tâches quotidiennes. Ainsi, ils accèdent directement au réseau de l'entreprise et à ses applications. Ceci ne va pas sans poser de nouveaux problèmes organisationnels et sécuritaires.

Sous l'effet de tous ces outils technologiques, les risques muent, mutent et évoluent beaucoup plus rapidement qu'auparavant.

Ainsi, la sécurité du système d'information contemporain est devenue si ce n'est un casse-tête, une tâche hautement complexe et changeante pour les spécialistes de la sécurité. De ce fait, le modèle classique de la sécurité dans lequel les équipes d'informaticiens qualifiés et compétents du département IT font face seules pour assurer l'entièreté de la sécurité d'entreprise doit être sérieusement repensé, voir intégralement refondu. Une intégration complète avec les différents départements, une participation accrue avec ses partenaires, fournisseurs etc. ainsi qu'une formation et surtout une sensibilisation des utilisateurs finaux et du help desk à ces problèmes est devenue plus que jamais nécessaire.

Il est aujourd'hui possible avec son téléphone mobile de partager quasi instantanément n'importe quel contenu et de fusionner des informations à partir de différentes plateformes (ce qu'on appelle généralement du *mashup*). N'importe qui peut prendre des photos ou des enregistrements sur son lieu de travail d'à peu près n'importe quel contenu ou informations sensibles et le diffuser en temps réel sans nécessairement avoir conscience du danger que cela représente. De plus, des outils comme les moteurs de recherche qui ont fortement contribués à populariser et démocratiser le Web sont venus en clé de voûte de ces menaces. Il est facile pour quiconque faisant preuve d'un peu de persévérance de trouver photos, coordonnées, documents etc., (certains sites Web comme www.123people.ch ou encore www.copainsdavant.com se sont spécialisés dans la recherche et/ou l'agrégation d'informations personnelles. Rien de plus facile alors pour l'internaute lambda de trouver ce qu'il cherche.). Le Web et ses technologies associées sont ainsi des canaux privilégiés pour la fuite d'informations et/ou la divulgation de données personnelles et professionnelles. Tous ces éléments facilitent alors considérablement le travail de l'ingénieur social et lui confèrent une puissance inégalée jusqu'à lors. L'exemple qui suit est une illustration parfaite de comment les médias sociaux et le Web peuvent aider à lancer une attaque :

> *« A mass spamming email specifically aimed at human resource staff with an attached résumé and the request : 'Please review my CV'. The CV is disguised as a zip file and contains the Oficia bot. This in turn downloads and installs the rogue AV package known as Security Essentials 2010. HR departement are used to receiving CVs over email, and this kind of malicious activity is indicative of the modern-day hacker. […] fraudsters know they can infect more computers, and steal more data, if they use techniques that fit the target. These attacks show the beginning of a move from undiscriminating mass malicious spam to a more targetted and direct form of social engineering. The key that unlocks targetted*

attacks is Web 2.0 in general, and social networking in particular. Social networks are just magic for the bad guys. (Townsend, 2010, p.34)

Voilà comment aujourd'hui, les médias sociaux et l'explosion du Web sont devenus des catalyseurs et des vecteurs hautement puissants de ce type de risque : *le social engineering*. Ces nouveaux outils ont modifié la perception, la physionomie et la mise en œuvre de la sécurité en entreprise.

4.1.1 Une politique pour encadrer

Les employés d'aujourd'hui sont connectés en permanence que ce soit à l'intérieur ou à l'extérieur du cadre d'entreprise et sont, de ce fait, de plus en plus familier avec les nouvelles technologies. Il n'est dès lors pas surprenant de constater que l'utilisation de ces mêmes outils devient de plus en plus répandue dans la sphère professionnelle. Toutefois, si une entité souhaite profiter des atouts certains que ceux-ci peuvent lui apporter, tout en encadrant et assurant une bonne gestion des risques tel que : risque d'image, risque légal etc., et une mitigation efficace vis-à-vis du risque de *social engineering*, une entreprise contemporaine doit dans sa boîte à outil de contremesures, mettre en place une politique des médias sociaux pour les encadrer.

Pour que ce document puisse vraiment être utile à l'employé, c'est-à-dire l'aider à comprendre les enjeux sécuritaires qui sont associés à ces technologies, et donc le sensibiliser et le responsabiliser, tout en lui permettant de pouvoir bénéficier de ces éléments, nous pensons que le document s'articuler autour de trois axes majeurs dans sa mise en œuvre :

1. Expliquer quels sont les risques spécifiques associés à chaque plateforme.
2. Élaborer une politique judicieuse qui permet un accès intelligent à ces ressources en fonction des attentes, des besoins, du positionnement et de la vision stratégique du management.
3. Éduquer, sensibiliser et faire participer les usagers pour augmenter leur prise de conscience liée aux risques. Et ainsi inciter un plus grand respect (une plus grande participation) vis-à-vis de la politique.

De façon plus spécifique, la politique doit permettre de savoir clairement ce que l'entreprise permet ou ne permet pas de faire en ligne, ce que les employés et éventuellement le public (c'est-à-dire monsieur et madame tout le monde, si l'entreprise possède une ou plusieurs plateformes publiques), sont autorisés ou non à écrire, dire ou faire. Ainsi, elle détermine une structure et une ligne de conduite en mettant des limites claires, en définissant le comportement attendu dans l'utilisation de ces outils et en expliquant quelles sont les conséquences en cas de non-respect de

cette dernière. Plus explicitement, cette politique elle devrait au moins comprendre les points suivants :

Ce que les employés peuvent ou ne peuvent pas faire :

Il s'agit dans cette section d'établir de manière claire et compréhensible, la conduite attendue et les lignes directrices claires quant au comportement des employés à l'égard de ces outils. Il faut également définir les bonnes pratiques qui permettront d'atténuer les risques de sécurité en ligne.

Le public et l'utilisation de (des) plateforme(s) de l'entreprise :

De plus en plus d'entreprises permettent aux prospects et différents membres du public d'intervenir sur leurs plateformes. Dans ce cas, la politique doit définir aussi clairement que possible quelles sont les attentes quant à l'utilisation de ces outils. Il faut notamment spécifier les actions qui peuvent être prises à l'encontre de l'usager lui-même et/ou du contenu publié en cas de violation des règles (retrait de contenu, avertissement, radiation de la zone membre etc.).

Ce que l'entreprise permet ou ne permet pas :

Le management devrait notamment expliquer comment il entrevoit l'utilisation des médias sociaux dans sa vision et sa stratégie d'entreprise (notamment en termes de développement de ses activités commerciales, de son image etc.). Plus particulièrement, il devrait préciser comment ceux-ci peuvent contribuer (bénéficier) à la croissance du business tout en contenant les risques.

Comme nous venons de le faire remarquer, une partie importante de ce document consiste à poser un cadre et des limites claires. Ceci permet un emploi judicieux des outils mentionnées et de donner une direction à l'ensemble des parties prenantes (employeur, employés et/ou membres du public). Dans ce contexte, il faut alors définir clairement le périmètre, c'est-à-dire le champ d'application de la politique. Pour cela, il est nécessaire de répondre et de se poser certaines questions comme par exemple :

- Qu'est-ce qui constitue une activité relevant des médias sociaux?
- Quelle serait une utilisation appropriée des médias sociaux dans l'entreprise?
- Devons-nous également inclure certains outils interne de l'entreprise (exemple: forum d'entreprise), dans cette politique?
- Qu'en est-il des usagers externes?

Dans ce questionnement, il est aussi important de tenir compte des autres acteurs clés de l'entreprise : les différents départements, les partenaires extérieurs etc. Leur implication et une élaboration commune du document va permettre une plus grande acceptation et une adhésion renforcée à la politique de l'entreprise dans son ensemble. Ainsi, la gestion des risques s'en voit renforcée et devient l'affaire de toute l'entité. De plus, suivant la taille et les besoins de l'entreprise, il peut être nécessaire et judicieux de se poser la question de savoir s'il ne faudrait pas développer une politique tout public d'une part, un document à usage interne d'autre part. A priori, les besoins, l'utilisation, les règles d'encadrement et donc les attentes ne sont pas les mêmes en fonction de la nature différente (interne, externe) des acteurs concernés.

Toujours dans cette optique, le document devrait couvrir trois (ou quatre selon les cas) des catégories suivantes :

Les lignes directrices générales:

Cette partie indique comment les médias sociaux sont perçus par l'entreprise, ce qui est attendu d'un employé dans son utilisation et quelles sont les conséquences en cas de non-respect de ces lignes directrices.

- ***Exemples :***

General subject	Guideline subject	Guideline example
Acceptable use of social media	Are there any company-imposed restrictions on social media activities while at work?	"Employees are expected to use social media for business purposes. Recreational use of social media is prohibited, and violators of this policy may face access restrictions based on time of day or bandwidth quota."
		"Employees are allowed unrestricted Internet access only during specific times in the day."
Security best practices	How should users deal with URL links?	"Exercise extreme caution when following any URL links posted by a third party or sent through a social media messaging service. Do not follow links unless they come from a known, trusted source."

Tableau 2 - Exemples de lignes directrices générales. Source: Forrester Research, Inc. *Your Anti-Social Behavior Stops Here — Set Guidelines To Adopt Social Media And Reduce Risk.* Cambridge (Massachusetts) – USA, 2011. pp. 7-8

Des lignes directrices relatives aux contenus postés par les employés:

Ces lignes directrices donnent les orientations précises et la façon dont un employé de la compagnie est autorisé à poster du contenu. Elles devraient également spécifier si le personnel peut utiliser (et dans quelles conditions), la raison sociale, le logo etc.

- ***Exemples :***

Employee posting subject	**Guideline subject**	**Guideline example**
Privacy	What are best practices for dealing with private or confidential information?	"Employees may not use or disclose any customer- or partner-identifiable information of any kind on any social media without the express written permission of the customer or partner."
Content policy	What content and information are users forbidden to post? What content are users forbidden to comment on?	"Employees are prohibited to comment on ongoing legal matters or disclose company confidential information."
		"Employees may not comment on matters related to the company's financial state."
		"Employees are advised not to post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to another person or entity. On company-hosted sites, employees are prohibited to post such materials."

Tableau 3 - Exemples de lignes directrices relatives aux contenus postés par les employés. Source: Forrester Research, Inc. *Your Anti-Social Behavior Stops Here — Set Guidelines To Adopt Social Media And Reduce Risk.* Cambridge (Massachusetts) – USA, 2011. p.9

Comportement en ligne:

La compagnie indique ici quel est le comportement attendu de la part de ses employés dans leurs interactions avec d'autres personnes en ligne. Elle devrait notamment expliquer la meilleure façon de répondre à des commentaires négatifs ou diffamatoires ainsi que les meilleures pratiques pour gérer d'éventuels contenus suspects (liens URL, pièces jointes etc.)

- ***Exemples :***

Online interaction subject	**Guideline subject**	**Guideline example**
Handling negative comments and inflammatory interactions	What constitutes appropriate language and manner in a confrontational situation?	"An employee cannot post derogatory remarks toward another in a public forum or engage in inflammatory, rude, irrelevant, insensitive, or generally inappropriate commentaries."
	What are best practices for dealing with negative views/opinions?	"Acknowledge the comment, formulate a polite response with facts, or agree to disagree."
	What are best practices for dealing with repeat offenders?	"Stop engaging. Report to site operator."
Safe online behavior	What are best practices for following hyperlinks and downloading applications?	"Do not follow URLs or download applications from untrusted sources. Double-check the source before downloading any software."

Tableau 4 - Exemples de lignes directrices pour le comportement en ligne. Source: Forrester Research, Inc. *Your Anti-Social Behavior Stops Here — Set Guidelines To Adopt Social Media And Reduce Risk.* Cambridge (Massachusetts) – USA, 2011. p. 10

Lignes directrices à l'attention du public (optionnel):

Si besoin, la compagnie devrait mettre sur pied un ensemble de lignes directrices, qui gouvernent le comportement et l'usage des membres du public, quant à l'utilisation de ses plateformes numériques en libre accès. En spécifiant également quelles sont les conséquences d'une infraction à ces règles.

- ***Exemples :***

Public user subject	Guideline subject	Guideline example
Appropriate use of the site	What will you allow members of the public to do on your social media site?	"Individuals using company- or affiliatesponsored online communities should refrain from using copyrighted material (written, audio, video, and all other electronic forms), as well as language that is obscene, defamatory, derogatory, profane, libelous, threatening, harassing, abusive, hateful, or humiliating to another person or entity."
		"We expect and encourage on-topic commentary and reserve the right to delete and discontinue any comments that veer too far away from relevant topics of discussion."
		"We will disable hyperlinks in useruploaded content."
		"We will not allow comments that appear to be spam."

Tableau 5 - Exemples de lignes directrices à l'attention du public. Source: Forrester Research, Inc. *Your Anti-Social Behavior Stops Here — Set Guidelines To Adopt Social Media And Reduce Risk.* Cambridge (Massachusetts) – USA, 2011. p. 11

Il faut garder à l'esprit qu'aussi judicieuse et pertinente que puisse être la politique, il est primordial de la communiquer et de l'exercer régulièrement auprès de ses employés. C'est la seule façon de garantir les éléments suivants :

1. Une forte compréhension et implication du personnel dans l'architecture sécuritaire de l'entité.
2. Permettre à ce document de devenir ainsi l'un de vos piliers de la sécurité en entreprise.
3. Constituer par ce biais, une première ligne de défense solide en impliquant directement les utilisateurs finaux et le help desk.

Même si la politique est strictement appliquée, il est important de garder à l'esprit que les nouvelles technologies évoluent très rapidement. Par conséquent le document doit aussi être régulièrement actualisé en fonction des besoins. Une révision annuelle devrait amplement suffire à moins que des changements importants interviennent en cours d'année. Dans ce dernier cas, une mise au point semestrielle peut s'avérer nécessaire. Selon la taille de l'entreprise, ses objectifs et la nature des plateformes dont elle dispose, un staff dédié peut être créé dans l'équipe de sécurité pour répondre et gérer les différentes problématiques liées à l'usage de ces outils.

Enfin, comme nous le discuterons en détails plus bas, une bonne politique n'est rien si elle n'est pas associée à un programme de formation et de sensibilisation régulier des ses employés vis-à-vis de ce risque.

4.1.1.1 Facebook, Twitter et compagnie

Le nombre de vols d'identité, de logiciels malveillants, de la perte ou du vol de données ainsi que des attaques ciblées ne cesse d'augmenter. Ceci est dû en grande majorité à des outils comme ceux figurant dans l'en-tête de ce chapitre. Les ingénieurs sociaux l'ont bien compris et c'est pour ces raisons que ces nouvelles technologies constituent un terreau fertile pour ceux cherchant des informations en vue d'une attaque ultérieure ou carrément pour lancer l'offensive elle-même.

On ne compte plus le nombre de comptes piratés sur ces plateformes. Imaginez alors les dégâts possibles : perte de l'image de la marque, perte de la confiance des clients, vol de données etc. Il est encore plus facile avec certaines plateformes de créer un compte fictif (que ce soit un compte corporatif comme par exemple avec *LinkedIn* ou un compte simple usager quelconque avec *Facebook*), puisqu'aucun véritable contrôle sur la véracité ou non d'un profil (c'est-à-dire des informations fournies) n'est mis en place par ces firmes au moment de l'ouverture d'un compte. Ajoutez-y une petite recherche avec *Google* pour compléter le profil malicieux (exemple : une fausse image de soi, de locaux etc.), rédiger une adresse, des emplois bidons, abonnez-vous à deux-trois pages de votre intérêt et le tour est joué. Certains n'hésitent pas à directement créer un vrai faux compte en s'inspirant directement du logo ou du matériel audiovisuel d'une entreprise existante.

Rien de plus facile par la suite d'inonder la toile avec du contenu malicieux ou de lancer une attaque par *phishing* en postant des liens URL piégés (typiquement sur *Twitter*). Vous obtenez alors des menaces sérieuses pour le système d'information. Si nous regardons d'un peu plus près, voilà ce que nous pouvons en tirer comme analyse pour les principaux d'entre eux :

Facebook:

Les principaux problèmes avec cette plateforme sont au nombre de trois :

1. La facilité avec laquelle il est possible de créer un profil malicieux pour ensuite lancer des attaques par *phishing* et/ou en la dissémination de logiciels malveillants
2. Il représente une vraie mine d'or d'informations directement exploitables par les fraudeurs, pirates etc. Car bien souvent, par méconnaissance des dangers ou simplement pour s'offrir une vitrine sur le Web, les gens n'hésitent pas à étaler plus d'informations que nécessaire. Dans le cadre d'entreprise ceci peut représenter un réel danger si les personnes ne savent pas quelles sont les limites à la distribution et la publication des informations.
3. Le dernier point est parfaitement résumé par *Chenxi Wang*[36] dans son rapport :

   « Another problem Facebook users often encounter is third-party applications. Using Facebook's application programming interface (API), third-party entities can produce Facebook applications that fulfill a small (but sometimes interesting) function such as virtual gift-giving or game-playing. These third party applications are not affiliated with Facebook and may present a security risk if let into your corporate environment. » (Chenxi Wang, 2010, p.4)

Twitter:

Dans le cadre de cet outil, les risques sont sensiblement les mêmes qu'avec *Facebook* (mine d'information, faux compte), mais il se présentent sous un autre angle. Voici ces caractéristiques principales :

1. De la même manière qu'avec son cousin *Facebook*, il est tout aussi aisé de créer un compte frauduleux. *Twitter* a toutefois la particularité de ne permettre à ses utilisateurs de poster que messages n'excédant pas les 140 caractères. Beaucoup d'informations sont alors transmises par le biais de liens URL. Rien de plus simple alors de faire circuler des liens malicieux pour lancer une attaque par *phishing*.

36 Chenxi Wang : *To Facebook Or Not To Facebook.* Forrester Research, Inc. Cambridge (Massachusetts) – USA, 2010, p. 4

2. Ce dernier est également constitué de plusieurs services d'agrégation de l'information[37], qui sont une pierre angulaire d'un vrai réseau social. Par ce biais, il garantit que les sources d'informations qu'il emploie sont de confiance. En plus de ses services, *Twitter* publie également une API[38] qui permet aux agrégateurs tiers d'inclure des tweets[39]. Et, c'est là que réside le problème : l'agrégateur est un tiers neutre, il ne discerne pas entre un utilisateur de *Twitter* légitime et un compte bidon dont les tweets peuvent potentiellement véhiculer des URL malveillantes!

LinkedIn:

Ce dernier est le leader dans le domaine des réseaux sociaux professionnels. Mais il offre également une mine de données sur les compagnies, leurs employés etc. Voici les principales faiblesses de cet outil:

1. Comme tout autre réseau social, *LinkedIn* n'a pas de moyens fiables à sa disposition pour vérifier si des personnes se listant comme des employés de chez *Nestlé* par exemple sont en effet des employés de ce groupe.
2. Tout comme les autres, s'il n'est pas utilisé judicieusement et que les informations publiées ne sont pas correctement filtrées par l'entreprise, il peut être utilisé comme plateforme d'attaque. En voici une parfaite illustration :

   « Take LinkedIn. One of the things you can do is get a company profile. This is effectively a corporate directory of that company – a list of everybody on LinkedIn that works for that company, with job title, and even those who have just joined the company. It is easy for a hacker to forge an email that appears to come from the head of HR to all new employees saying, 'Welcome, congrats on joining our company. Click on this link to our company intranet and find out about all the wonderful advantages and opportunities'. It would, of course, be a false website containing drive-by malware. » (Townsend, 2010, p.34)

Nous pourrions continuer ainsi avec bon nombre de plateformes. Le but ici n'est pas de dissuader quiconque d'utiliser ces outils, et encore moins de mettre uniquement en exergue leurs faiblesses. Tout système a ses failles, mais aussi ses forces et nous croyons profondément utile d'en avoir conscience, et d'attirer sur celles-ci l'attention des décideurs, qui, un jour, devront peser le pour et le contre de ces technologies dans la gestion de leur appareil sécuritaire.

Ce que ces exemples montrent, c'est que l'utilisation de tels outils au quotidien dans un cadre entrepreneurial demande une attention et une gestion toute particulière.

---

37 Cf. glossaire p.81

38 Cf. glossaire p.81

39 Il s'agit du nom usuel donné aux messages postés sur cette plateforme.

Typiquement dans le cas de *LinkedIn*, il est important pour l'entité de s'assurer de qui adhère à son compte, de retirer d'anciens employés (faute de quoi, il serait possible de garder l'accès à des informations potentiellement dommageables) etc. Malgré toute la bonne volonté et une politique encadrante, il faut garder à l'esprit que ces outils sont très souvent externes à l'entreprise et donc gérés par d'autres sociétés, souvent des *start-ups*. Ceci signifie donc pour celui qui les emploie, qu'il n'aura qu'un contrôle relativement partiel sur ces derniers, et qu'il ne lui sera pas possible d'appliquer la même politique que celle qu'il peut appliquer chez lui. De plus, comme la popularité et la croissance de ces technologies s'accélèrent, notamment envers les usagers du Web, il devient primordial que les professionnels de la sécurité restent attentifs et vigilants envers ces outils.

Enfin, comme nous aimons à le rappeler, la formation joue un rôle central dans cette approche. Il est nécessaire de rendre attentif l'utilisateur à ne pas suivre bêtement quelqu'un sur *Twitter* simplement parce qu'il nous suit, sur *Facebook* d'installer n'importe quel jeu ou application, sur *LinkedIn* de croire naïvement aux déclarations d'un individu à la simple vue de son parcours professionnel, de ne pas cliquer sur un lien qui semble trop beau pour être vrai; l'utilisateur doit garder l'esprit critique quant à leur usage. Et pourquoi pas donner aux utilisateurs les moyens d'agir, notamment en mettant en place un processus d'escalade clair dans la politique pour les impliquer dans ce maillon de la sécurité.

4.2 Les moteurs de recherche

Tout comme les réseaux sociaux, les moteurs de recherche au premier titre desquels : *Google*, sont des outils de plus en plus employés par les pirates pour glaner toute sorte d'informations. Que ce soit des documents, des fichiers audios ou vidéos en passant par la recherche de logiciels, ce sont de véritables cavernes d'Ali Baba pour ceux qui veulent lancer une attaque d'ingénierie sociale des plus efficaces.

Un bon mot-clé, une chaîne de caractères bien choisis dans la barre de recherche du moteur de recherche et le tour est joué. Une requête peut être construite avec des opérateurs logiques et de nombreux opérateurs spécifiques proposés par les différents moteurs de recherche.

L'ingénieur social peut ainsi cibler sa recherche et exploiter la mine d'informations récoltées par ce biais pour atteindre ses objectifs. Voici par exemple les opérateurs proposés par *Google*[40] :

Tableau 11-1 : Opérateurs compatibles

Service de Google	Opérateurs
Web	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, inlink:, phonebook:, related:, rphonebook:, site:, stocks:
Images	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Groupes	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Annuaires	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
Actualités	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:
Froogle	allintext:, allintitle:, store:

Figure 6 - Exemples d'opérateurs pour la recherche d'informations sous *Google*. Ils sont présentés ici classés par service. Source : GOMEZ-URBINA, Alexandre : *Hacking Interdit 4ème édition*. Micro Application. Paris : 2010, p. 385

Il est bien sûr possible de les combiner tous ces opérateurs entre eux pour affiner la recherche à volonté. Prenons par exemple l'opérateur *filetype:*. Dans le contexte du service Web, il permet la recherche de documents sur la base d'une extension spécifique : *filetype:pdf* (documents PDF), *filetype:docx* (documents Word), *filetype:xslt* (documents Excel) etc. Si vous le combine avec l'opérateur *site:* vous pouvez imaginer une requête de ce genre : « *site:microsoft.com filetype:pdf* ». Celle-ci vous retourne alors tous les documents avec l'extension *.pdf* appartenant au domaine *microsoft.com*. En tant que pirate, vous pourriez sans difficulté remplacer ce nom de domaine par celui d'une entreprise que vous cherchez à cibler. Une véritable mine d'informations s'offre alors à vous, il ne reste plus qu'à vous servir.

40 Le site web suivant : www.googleguide.com/advanced_operators.html offre une liste impressionnante d'opérateurs avec leur explication respective. Des exemples d'emploi sont également proposés.

D'autres combinaisons sont illustrées ci-dessous :

Requêtes	Description
project filetype:xls site:fr	Recherche tous les projets crées sous Excel sur des sites français.
secret ext:xls site:fr	Recherche des documents avec la dénomination *secret* et qui sont crées sous Excel sur des sites français.
confidentiel filetype:xls site:fr	Recherche des documents avec la dénomination *confidentiel* et qui sont crées sous Excel sur des sites français.
ext:xls personnel email	Recherche des fichiers Excel qui peuvent contenir des adresses du personnel, des adresses email et d'autres types d'informations sensibles.

Tableau 6 - Exemples de requêtes combinées pour la recherche d'informations sous Google.

De même, il existe bon nombre d'autres opérateurs et de requêtes combinées pour rechercher également des logiciels et leurs versions, des jeux, des routeurs etc[41].

Notre objectif n'est pas ici de donner une démonstration complète des outils de recherche et encore moins d'effectuer un cours sur les requêtes *Google*[42]. Le but est de sensibiliser le lecteur à cette problématique (car les moteurs de recherche n'oublient jamais) et plus particulièrement de rendre attentif celles et ceux qui ont la responsabilité de la sécurité du système d'information de leur entreprise. Il est plus que jamais primordial de mettre en place des mesures (techniques, politiques, formation etc.) pour prévenir la fuite d'information sensibles pour l'entreprise dans le domaine

41 Le chercheur *John Matherly* a ainsi mis au point un moteur de recherche qu'il a appelé *Shodan* (www.shodanhq.com) qui permet d'effectuer des recherches sur le Web pour des serveurs, des routeurs etc. Rien de plus facile d'effectuer alors une cartographie d'un site.

42 Deux ouvrages peuvent permettre au lecteur qui le souhaite d'aller plus loin dans cette thématique. Celui de *Johnny Long : Google Hacking for Penetration Testers* ou encore celui que nous citons en bibliographie de *Gomez-Urbina Alexandre : Hacking Interdit 4ème édition* (chapitre n°11 tout particulièrement).

public. La prévention est alors une pierre angulaire dans ce contexte et reste sans nul doute la meilleure des armes.

DEFCON 20 Social-Engineer.Org SECTF Flag List			
Logistics	**Pts**	**Company Wide Tech**	**Pts**
Is IT Support handled in house or outsourced?	5	What operating system is in use?	10
Who do they use for delivering packages?	7	What service pack/Version?	15
Do you have a cafeteria?	5	What program do they use to open PDF documents and what version?	10
Who does the food service?	7	What browser do they use?	10
Do you use disk encryption? If so which type?	7	What version of that browser?	15
Other Tech		What mail client is used?	10
Is there a company VPN?	7	What version of the mail client?	10
Do you block websites? (Facebook, EBay, etc)	3	Fake URL(getting the target to go to a URL)	25
Is wireless in use on site?	3	**Employee Specific Info**	
ESSID Name?	7	How long have they worked for the company?	5
What make and model of computer do they use?	5	What days of the month do they get paid?	5
What anti-virus system is used?	10	Employee termination process?	5
Can Be Used for Onsite Pretext		New hire orientation information?	3
Do you have a cleaning/janitorial service?	5	Employees schedule information	5
What is the name of the cleaning/janitorial service?	7	- (start/end times, breaks, lunches)	5
Do you have a bug/pest extermination contract	5	Do they have a PBX system?	5
With Whom?	7	What sort of phone system is used?	7
What is the name of the company responsible for the vending machines onsite?	7	When was the last time they had awareness training?	10
Do they have trash handling?	5		
Who handles their trash/dumpster disposal?	7		
Do you have a 3rd party security guard company?	9		
Who is it?	10		

Figure 7 - Exemples d'informations récoltées via la recherche passive. Toutes ces informations ont pu être trouvées via les moteurs de recherche et les réseaux sociaux. Le nombre de points indique, la valeur de chaque pièce d'information dans le cadre du test de pénétration en ingénierie social mené lors de la conférence. Source : HADNAGY Christopher : *Social Engineering Capture the Flags Results – Defcon 20*. 2012, p. 8

En effet, une fois l'information diffusée sur la toile, il est très difficile (voir quasi impossible) de la retirer. Il ne vous reste alors plus qu'à écrire au moteur de recherche concerné en espérant qu'il puisse désindexer la (les) page(s) problématiques. Une réflexion et une sensibilisation à cette problématique doit alors être menée en entreprise sur comment, quoi et quand publier telle ou telle information. Le contenu qu'une entreprise décide de rendre accessible via son site Web, ses diverses plateformes numériques peut avoir une incidence importante sur sa sécurité.

La Figure 7 ci-dessus illustre de façon concrète la menace que ceci peut représenter ; il s'agit des informations que les équipes M. HADNAGY Christopher[43] ont pu glaner avec des outils comme les moteurs de recherche et les réseaux sociaux lors de la tenue du DEFCON-20.

Voici alors la conclusion qu'il en tire après analyse de l'exercice dans son ensemble :

> *« […] leakage information into the public domain is a big problem for companies. The fact that most flags could be obtained through publicy available information speaks volumes to the problem. Companies and their employees are primarily responsible for this leakage. Often these leaks were not due to confidential documents or ex-employees, but well meaning employees tweeting or blogging about things on LinkedIn or the social media sites. […] »*[44]

Bien sur tout ce que nous venons de décrire n'est pas uniquement valable pour *Google* : cela s'applique évidemment aussi à *Bing*, *Yahoo* etc.

Un dernier point sur lequel il nous semble important d'attirer l'attention du lecteur en matière de moteur recherche est parfaitement expliqué par Mr. TOWNSEND Kevin dans son article :

> *« A more subtle variation uses the technique known as 'search engine poisoning'. This will likely involve a specially crafted website that contains malware. As soon as an incident of international interest occurs, the attackers use search engine optimisation techniques to make this website appear high on search engine returns. So, if there's an earthquake or plane crash – or an ash cloud that gets your interest – use caution when searching in Google, Bing or Yahoo ; there may be false links to a bad website. » (Townsend, 2010, p.33)*

Au final, comme nous avons pu le voir avec les médias sociaux, les moteurs de recherche sont de redoutables outils au service de l'ingénieur social. Il faut alors prendre les bonnes mesures pour sensibiliser les utilisateurs à ces problématiques. Trop souvent par inadvertance ou ignorance, ces derniers divulguent de précieuses informations qui ne devraient pas se trouver sur la toile. La fuite d'information constitue un véritable problème qu'il s'agit de prendre au sérieux dans ce contexte. D'autre part, il est également de la responsabilité de l'entreprise de régulièrement s'assurer que les données se trouvant sur sa (ses) plateforme(s) public(s) représentent un niveau

---

43 Le tableau est directement tiré du rapport: *Social Engineering Capture the Flags Results – Defcon 20* écrit par *M. HADNAGY Christopher.* Le document peut être consulté à l'adresse suivante : http://www.social-engineer.org, via l'onglet CTF du menu principal en haut de la page d'accueil.

44 La citation est tirée du document : *Engineering Capture the Flags Results – Defcon 20* écrit par *M. HADNAGY Christopher* en p. 15. Le document peut être consulté à l'adresse suivante : http://www.social-engineer.org, via l'onglet CTF du menu principal en haut de la page d'accueil.

acceptable de prise de risque pour elle. Et ceci passe notamment par la revue périodique de ses contenus. En parallèle à ces éléments, il est aussi important de définir des processus et procédures claires pour atténuer le risque. Et permettre à l'employé se trouvant éventuellement sous la menace de ce type d'individu, de prendre la bonne décision et lui donner les moyens d'agir le cas échéant (typiquement le cas de la secrétaire qui ne connaît pas les règles en cas de personne suspecte au téléphone). Enfin, l'efficacité des mesures mises en place doit impérativement être testée et approuvée de façon régulière :

> *« Perhaps worst of all, the effectiveness of controls and procedures are never validated. They are put in place and left alone under the assumption that all shall be well. Hence the continuing cycle of exploitation. » (Beaver, 2009, p.35)*

4.3 Techniques courantes

En plus de ce que nous venons d'exposer et d'illustrer dans les précédentes pages de ce chapitre, il existe un certain nombre de techniques courantes d'ingénierie sociale dont voici un aperçu : De manière à être le plus clair possible, cette section sera présentée en deux temps. Dans un premier temps, un graphique globale avec les principales techniques répertoriées et leur désignation respective (les noms seront donnés en anglais pour l'ensemble des techniques. Ceci est dû essentiellement au fait qu'ils apparaissent sous cette forme dans la littérature spécialisée).

Enfin, en second lieu, un descriptif plus poussé qui permettra d'avoir les éléments suivant en plus du nom de la technique: *sa description* et *la (les) contremesure(s) existante(s)*.

Figure 8 - Liste des principales techniques d'ingénierie sociale.

Description des techniques et contremesure(s) :

1. *Shoulder surfing*

a. Description

L'attaquant fait ici appel à des méthodes d'observation, comme par exemple regarder par-dessus l'épaule d'un individu pour obtenir des informations alors qu'il est en train d'effectuer des actions où l'utilisation de données sensibles est nécessaire (typiquement mot de passe). Elle nécessite une grande proximité avec la cible. Dans certain cas, il peut faire appel à des dispositifs de vue à distance (jumelles, web-cams, etc.).

Il faut se méfier si on cherche à vous distraire (prétexte d'une discussion urgente, objet laissé tomber à terre etc.) au moment d'actions sensibles.

b. Contremesures

- Mise en place d'un système de double authentification.

- Avoir une politique forte en matière de mot de passe (nombre minimum de caractères, mélanger chiffres & lettres etc.).
- Veiller à ce que personne ne soit en train de vous observer dans une situation délicate.

2. Dumpster Diving

a. Description

La fouille des poubelles est également un moyen efficace pour trouver des informations (n° de compte client, n° de téléphone, adresse etc.). C'est souvent un bon moyen pour usurper l'identité d'un individu. Sans compter que les compagnies se débarrassent également des vieux manuels, organigrammes, des impressions de données sensibles, des noms de connexion ou de mots de passe etc. Pour celui qui sait fouiller et valoriser ces informations, il peut y trouver le début d'un bon scénario.

b. Contremesures

- Faire usage des broyeurs pour les documents papier à caractère confidentiel.
- Définir et mettre en œuvre une politique sur le traitement des documents confidentiels (copies papiers ou électroniques).
- Restreindre les permissions d'impressions des documents sensibles à celles et ceux qui en ont les droits et le besoin.
- Décourager l'utilisation de copies papier.
- S'assurer que les impressions essentielles soient enfermées après utilisation.
- Les poubelles contenant les déchets sensibles doivent le cas échéant être fermées et stockées dans un local à l'abri des regards.

3. Search engines

a. Description

Comme nous l'avons vu dans nos pages précédentes, les moteurs de recherche sont des outils redoutables dans les mains d'un ingénieur social. Essentiels dans la récolte d'informations en vue de la construction d'un scénario, ils peuvent également être une plateforme de lancement pour une attaque. Pour plus de détails, veuillez vous référer au sous-chapitre 4.2, p.45

b. Contremesures

- Réaliser un audit de sécurité des informations publiées sur les plateformes de l'entreprise.
- Revoir régulièrement les informations publiées.
- Sensibiliser et former les collaborateurs à l'importance de l'information.

4. Social networks

a. Description

Au même titre que les moteurs de recherche, les réseaux sociaux sont des outils redoutables pour les pirates. Il faut donc les manier avec précautions et plus particulièrement dans un cadre d'entreprise. Pour plus de détails, veuillez vous référer au sous-chapitre 4.1 et suivants, p.33.

b. Contremesures

- Mettre en place une politique des médias sociaux.
- Sensibiliser et former les collaborateurs quant à l'utilisation de ces outils en entreprise.

5. Phishing

a. Description

Cette technique consiste essentiellement à faire croire à un courriel officiel (d'une banque, d'une administration publique etc.), dans le but de tromper le destinataire, soit en lui demandant de cliquer sur un lien falsifié, soit en lui demandant de remplir directement un formulaire pour récupérer des données sensibles (mot de passe, nom d'usager, etc.).

Il est également fréquent d'y joindre des pièces jointes malicieuses, qui permettront par la suite (une fois téléchargées) l'installation d'une porte dérobée par le pirate. L'emploi d'un site web falsifié (ou défacement[45]) est également une possibilité ; ce procéder est un excellent moyen pour voler une identité à des fins d'usurpation ultérieure. À noter que ce type de procédé cible généralement un grand nombre d'individus.

45 Cf. glossaire p.81

b. Contremesures

- S'assurer de la mise à jour régulière des anti-virus, firewall, filtres anti-spam et autre mesures techniques en entreprise.
- Ne jamais divulguer ou donner des informations sensibles sur sa personne ou concernant l'entreprise via un formulaire en ligne (qui plus est si la demande vous semble suspicieuse, ou incongrue).
- Former et éduquer le personnel en le rendant attentif à ces menaces notamment : en vérifiant la source du courriel, ne pas cliquer sur des liens suspects, éviter de télécharger des pièces dont on ne connaît pas la provenance etc.
- Mettre en place un processus d'escalade qui permet aux usagers de signaler d'éventuels incidents. Ainsi, des statistiques pourront être tenues et serviront de point d'amélioration.

6. Spear-phishing[46]

a. Description

Fonctionne sur les mêmes principes que ceux du *phishing*. Généralement les courriels piégés sont plus personnalisés et visent un petit groupe d'individus ou une personne unique.

b. Contremesures

- Cf. phishing

7. SMS-phishing

a. Description

Sur le même principe que le *phishing*, cette technique utilise les messages textes comme appât pour inciter les personnes à divulguer des informations personnelles. La méthode employée pour capturer des informations peut être une URL de site web falsifié. Mais, il est aussi fréquent de voir apparaître un numéro de téléphone qui se connecte à un système de réponse vocale automatisée. Généralement le message contient quelque chose qui attire l'attention immédiate de la cible :

« Nous confirmons que vous avez signé pour notre service de rencontres. Vous serez facturé 5 CHF par jour, sauf si vous annulez

46 Cf. glossaire p.81

immédiatement votre inscription en cliquant sue cette URL [ici l'URL piégée]. »

Ou :

« [Ici le nom d'un institut bancaire en ligne connu] confirme que vous avez acheté un ordinateur à partir [nom de la société informatique populaire] avec votre carte de crédit. Visitez cette URL si vous n'avez pas fait cet achat en ligne. Votre compte a été suspendu. Appelez immédiatement le : XXX-XX-XX pour réactiver votre compte.»

L'URL vous guide sur un site d'apparence légitime pour soutirer votre code de carte, numéro de client etc. De la même façon, le numéro de téléphone dirige l'usager vers un système de réponse vocale automatisé, semblable à celui utilisé par l'institution financière et qui vous demandera les mêmes informations.

b. Contremesures

- Ne jamais divulguer ou donner des informations sensibles sur sa personne ou concernant l'entreprise via un formulaire en ligne (qui plus est sir la demande vous semble suspicieuse, ou incongrue).
- Le cas échéant, contacter directement l'établissement pour s'avoir exactement de quoi il retourne.
- Vérifier le numéro de téléphone et/ou l'URL en s'assurant qu'ils proviennent d'une source fiable.

8. Infested devices

a. Description

Les périphériques malicieux (clés USB, CD-ROM et autres supports contenant des logiciels malveillants) et une technique simple et efficace pour introduire des logiciels espions (backdoors et autre cheveaux de Troie) afin de garder un œil sur sa cible et revenir ultérieurement si nécessaire.

b. Contremesures

- S'assurer de la mise à jour régulière des anti-virus, firewall, logiciels d'analyse de périphériques et autres mesures techniques en entreprise.
- Mettre à jour régulièrement les patchs de sécurité sur les machines des usagers.

- Sensibiliser et former les collaborateurs à cette problématique. Si des périphériques sont trouvés sans raisons apparentes, il peut être bon de les amener au service informatique ou à son supérieur hiérarchique, qui eux pourront prendre les dispositions nécessaires.
- On peut également interdire physiquement l'emploi des clés USB, CD-ROMs et autres cartes mémoire sur les postes de travail de l'entreprise. Soit en fournissant des postes dépourvus de tels lecteurs, soit en configurant les postes pour qu'il soit impossible de les employer.

9. Identity theft

a. Description

Le vol (ou usurpation) d'identité n'est pas une technique au sens stricte du terme. Elle représente toutefois, un excellent vecteur pour les pirates qui souhaitent gagner l'accès à un bâtiment ou soustraire des informations frauduleusement en se faisant passer pour un employé, un technicien etc. Elle s'appuie notamment sur des éléments comme la fouille des poubelles (*dumpster diving* ou encore le *phishing*). Ce type de procédé est en foret augmentation ces dernières années.

b. Contremesures

- Il peut être très difficile de déterminer si la personne revêt une vraie ou une fausse identité. C'est pourquoi, il est nécessaire de mettre en place des processus et des procédures strictes. Entre autre : vérifier les accréditations et les droits d'accès de la personne, mettre en place des éléments de sécurité physique[47] à l'entrée du bâtiment (badges et autres scanners corporels) ou encore vérifier les antécédents de la personne.
- En cas de doute ou d'empressement de l'individu, il peut être judicieux de poliment lui demander de patienter et ainsi remonter l'information à son supérieur hiérarchique. Le temps des vérifications d'usage.

---

47 Bien entendu, cet aspect n'est pas applicable en toutes circonstances. Il dépendra notamment des actifs que l'entreprise doit protéger, de son secteur d'activité et également de l'aspect financier. En effet, ces mesures techniques ont généralement un cout très important qu'il est important de prendre en considération au moment de la mise en place.

- Par téléphone, il est possible de gentiment prendre le téléphone de la personne est d'indiquer que nous la rappellerons dès que possible. Ceci laissera le temps au standard d'éventuellement vérifier les informations et/ou de faire remonter l'incident[48].

10. Telephone

a. Description

Les attaques per téléphone sont encore monnaie courante. En effet, il offre une grande simplicité d'action et l'anonymat. Ce sont là des atouts non négligeables pour un pirate. Un anonymat certain puisqu'il est possible de cacher son numéro ou de prendre des offres sans abonnement. Et simplicité puisqu'un appel peut se passer rapidement et qu'il n'y a pas de contact direct avec la cible. Il suffit alors de surveiller son ton de voix.

b. Contremesures

- Il est important de former son personnel à ne pas divulguer plus d'informations que nécessaire (typiquement le help desk, service après-vente etc.). Et entre autre, ne jamais donner des informations considérées comme sensible pour l'entreprise.
- Donnez les moyens à son personnel d'effectuer les vérifications d'usage en cas de suspicion, ou faire remonter l'information (processus d'escalade).

11. Postal service and fax

a. Description

Comme l'explique très bien M. MUSSET[49] :

« Le facsimilé et le courrier bénéficie d'une croyance voulant que puisque leur envoi n'est pas gratuit, contrairement à l'e-mail, les expéditeurs font preuve de sélection dans leurs campagnes d'envois. »

---

48 Il est primordial ici de donner la possibilité à l'employé d'agir sur sa tâche. Notamment en vérifiant les informations données, l'identité etc. Et de mettre en place un processus d'escalade qui le cas échéant lui permet de reporter l'incident à un supérieur. Par ailleurs, il ne faut jamais agir dans la précipitation.

49 L'extrait est directement tiré de l'ouvrage suivant :

- MUSSET, Jöelle : *Sécurité Informatique : Ethical Hacking : Apprendre l'attaque pour mieux se défendre*. Editions ENI. France : 2009, 355 p.52

Ceci d'autant plus si le pirate choisit une mise en page professionnelle, avec du papier en-tête soigné et des détails visuels saillants (logos de l'entreprise etc.). Ils permettent alors facilement une attaque à distance tout comme le téléphone et le courriel.

b. Contremesures

- En cas de doute il est possible d'appeler directement la compagnie, institut etc. supposé avoir fait l'envoi postal ou le fax pour vérifier si le document est bien légitime.
- Vérifier également en interne si l'entreprise est effectivement d'une manière ou d'une autre en affaire avec l'expéditeur supposé.
- Détruire le document si nécessaire.

12. TailGating

a. Description

Une excellente description de cette technique fréquemment employée est donnée par dans l'article *Wikipédia* en anglais traitant de l'ingénierie sociale[50] [consulté le 19 juin 2013]:

« An attacker, seeking entry to a restricted area secured by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access. Following common courtesy, the legitimate person will usually hold the door open for the attacker. The legitimate person may fail to ask for identification for any of several reasons, or may accept an assertion that the attacker has forgotten or lost the appropriate identity token. The attacker may also fake the action of presenting an identity token. »

Elle relève donc essentiellement du quiproquo.

b. Contremesures

- Toujours scrupuleusement vérifier les accès (badges etc.) du personnel. Ceci tout particulièrement lorsque l'accès à une zone sensible est requis.
- Vérifier (en cas d'oubli involontaire etc.) dans le registre du personnel que la personne existe bel et bien et possède les bons accès (validité des accès, que la personne n'a pas été licenciée etc.).

50 L'article au complet peut être consulté à cette adresse : http://en.wikipedia.org/wiki/Social_engineering_(security)

- En cas de suspicion faire remonter l'information et congédier la personne.

13. Face to face

a. Description

L'attaque en temps réel ou face à face est une technique qui permet essentiellement de manipuler la victime dans le but d'obtenir les informations et/ou biens convoités. Elle demande du sang-froid et notamment la capacité d'être maître de ses émotions. Notamment de contrôler les éventuelles crispations, micro-expressions ou tout autre signe de stress qui risque de trahir l'ingénieur social.

b. Contremesures

- Il n'existe malheureusement pas de solution miracle et devant un bon ingénieur social avec de l'expérience, qui connaît bien les leviers psychologiques et s'est bien renseigné sur la cible, la solution la meilleure reste : l'entraînement par des programmes de prévention, sensibilisation et formation régulier et adapter à ce risque spécifique. Il est nécessaire qu'un individu puisse identifier le fait qu'il soit sous la menace d'une telle attaque et qu'il puisse prendre les bonnes options pour y répondre.

14. Websites phishing

a. Description

Le défaçage de site Web (cf. glossaire sous défacement) est une technique employée fréquemment pour usurper l'identité d'une personne en lui soustrayant des informations confidentielles et personnelles. Elle est souvent combinée avec d'autres techniques (exemples : phishing, spear-phishing).

b. Contremesures

- Vérifier si l'URL du site Web en question est bien celle légitime. Très souvent entre le vrai site et celui falsifié, l'URL ne correspond pas tout à fait en tout point. On peut alors simplement la détecter à l'œil nu en regardant dans la barre de saisie du navigateur internet. Le cas échéant signaler l'incident au responsable.

- Ne jamais donner mot de passe, code d'accès ou toute autre information sensible sur sa personne ou sa compagnie par un formulaire en ligne.
- Mettre à jour les patchs de sécurité.
- Le cas échéant, le (les) serveur(s) Web de l'entreprise seront protégé adéquatement et notamment placé dans une DMZ[51] avec des filtres Web, pare-feu etc. vérifiant le trafic entrant et sortant qui souhaiteront accéder à ses services.

Nous avons ici discuté de quatorze techniques possibles d'ingénierie sociale. Il existe quelques variantes de ces dernières, mais les plus couramment mises en œuvre sont présentées dans nos pages. Comme le lecteur peut le constater, il existe dans certains cas des solutions techniques (anti-virus, pare-feu etc.), mais pour bon nombre d'entre elles, la sensibilisation et la formation adéquate du personnel revêt une importance toute particulière. Cette thématique fait justement l'objet d'un développement dans les pages qui suivent.

51 Cf. glossaire p.81, sous le terme *zone démilitarisée*

5. Formation, prévention et mitigation

5.1 La formation et la sensibilisation des employés

Comme nous l'avons laissé entrevoir tout au long du dernier chapitre, la formation, la sensibilisation et l'éducation du personnel sont des éléments incontournables de l'arsenal de mesures (contre-mesures) qui constituent la barrière défensive de l'entreprise. Ceci est vrai pour tout un ensemble de risques, mais l'est encore d'autant plus pour le *social engineering* :

- D'une part car comme nous l'avons souligné, il s'agit ici d'exploiter les failles humaines d'un individu (les bugs dans l'hardware humain)
- D'autre part, contrairement à toute une série de risques plus techniques, l'épicentre du problème (ce qui est pris pour cible en premier lieu) n'est plus le matériel (routeurs, serveurs etc.), mais l'humain en lui-même dans ce qu'il est, dans sa constitution intrinsèque. Il suffit pour s'en convaincre de regarder la partie concernant les biais cognitifs.

De ce fait, la sensibilisation et l'entraînement régulier sont des piliers fondamentaux puisqu'aucune machine, aucun pare-feu, aucun processus ne peut à l'heure actuelle repérer ou détecter la supercherie ou la manipulation psychologique des individus.

Il est non seulement important de former les personnes, mais également de mettre en place et de revoir sur une base régulière les contrôles, les processus et les procédures afin d'en évaluer l'efficacité et l'efficience. Par exemple, en disposant d'une politique des médias sociaux, d'un processus d'escalade avec des procédures claires qui permettent au standard téléphonique de vérifier des appels suspicieux et le cas échéant les faire remonter à qui de droit ou encore d'une politique sur la gestion des actifs informationnels (politique de l'information). Tout comme une politique de sécurité qui doit être révisée à intervalle régulier pour assurer son efficacité et sa bonne mise en œuvre, ces derniers le doivent également. En parallèle, des moyens techniques appropriés: patchs de mise à jour, antivirus etc. sont aussi nécessaires pour diminuer la surface d'attaque. Cependant, ces derniers aspects sont plus techniques et se passent généralement en toile de fond pour l'employé lambda (sans qu'il en ait conscience, ou qu'il est besoin de s'en préoccuper). Or, ici c'est lui qui est pris directement pour cible.

Les programmes de sensibilisation et de formation au *social engineering* sont nécessaires et ils doivent impérativement être mis en place. Ceci peut se faire de manière ludique. On peut imaginer qu'une entreprise organise une fois par année ou une fois par semestre (ou tous les trimestres dépendant de la taille et de l'importance

de l'entreprise, de son budget formation, de son exposition au risque ou encore de la stratégie du management), une journée du *social engineering*. Au cours de cette journée de sensibilisation, le personnel serait réparti par département. Un certain nombre d'entre eux (par exemple entre deux et quatre individus) seraient tirés au hasard et à l'insu de leurs collègues, pour un département donné et ce par leur supérieur hiérarchique. Ces personnes occupent le temps d'une journée, le rôle d'ingénieur social avec pour mission de réussir à dérober à leurs collègues toutes informations susceptibles de leur permettre une escalade de privilèges (mot passe, droit d'accès etc.). À contrario, le reste des personnes endosseraient par défaut le rôle de cibles potentielles. Pour chaque information glanée, un certain nombre de points lui est attribuée. À la fin de cette journée, on présente les résultats par département (RH, Comptabilité, Recherche et Développement etc.). Le gagnant (département qui a le score le plus faible, c'est-à-dire celui dont le personnel a divulgué le moins d'informations) est distingué et son titre est remis en jeu l'année suivante. Ce type de procédé présente deux grands avantages :

1. Permet de repérer les faiblesses département par département et de mieux cibler, adapter la prévention, formation, sensibilisation en conséquences.
2. Les personnes retiennent mieux l'information si elles sont associées (parties prenantes) au processus, s'il y a un but ou une émotion qui inscrit durablement ces éléments dans la mémoire. Le jeu de rôle permet tout ceci.

La contrepartie est que les départements avec les scores les moins bons risquent de se sentir stigmatiser. Il est alors primordial que l'équipe en charge de cette activité, prenne le temps d'expliquer aux employés qu'il ne s'agit pas d'un concours permanent entre eux. Mais, une évaluation sous forme pratique et participative et à intervalle régulier, de la qualité de la formation et sensibilisation à ce risque que le service dispense à tous les employés. Leurs remarques et critiques peuvent être prises en considération lors du débriefing pour améliorations futures. Il est important d'impliquer les personnes dans ce processus si on souhaite qu'elles se sentent concernées par le problème. De cette façon, une amélioration de la sécurité peut être ressentie sur l'ensemble de la structure.

Le référentiel le plus connu en matière de système de gestion de la sécurité de l'information, qui est aujourd'hui une norme internationale, est celui de l'*ISO 27001*[52]. Bien que très employé notamment dans l'aide à la constitution d'une politique de sécurité, il peut se montrer quelque peu rébarbatif, surtout pour sensibiliser des employés dont le cœur de métier n'est pas la sécurité à proprement parler. D'autres référentiels plus accessibles (comme par exemple *CORAS*[53]) permettent d'aborder la question des risques et de la sécurité sous un angle plus décontracté ce qui peut permettre une meilleure intégration chez les employés. D'autre part, il est aussi possible d'imaginer à intervalle régulier des séminaires de formation ludiques et didactiques en entreprise sous la forme de petits jeux d'équipe. Chaque équipe est constituée de cinq à sept personnes (soit du même département ou des équipes mixtes, ce qui a l'avantage d'attirer l'attention des uns et des autres sur certaines petites particularités en fonction du poste). Le formateur leur transmet un cas pratique par écrit d'ingénierie sociale où ils doivent identifier le (les) vecteurs d'attaque et trouver les mesures de mitigation adéquates. Au bout d'une demi-heure – quarante minutes, le groupe fait un petit exposé au reste des collègues. Ceci favorise l'échange d'idées et la mise en application des concepts appris; le formateur peut voir si les notions sont correctement intégrées et une mise à niveau peut se faire si nécessaire (nouvelles techniques, corrections etc.).

Dans tous les cas, il faut être inventif, imaginatif, impliquer les personnes concernées et, pourquoi pas, sortir des sentiers battus. Trop souvent, la sensibilisation à la sécurité est vécue comme un exercice monotone ou pire encore, elle représente une obligation (cadre légale, législation etc.) que l'on s'empresse d'expédier. Forcer ses employés une fois par année à se réunir dans la salle de conférence pour suivre un séminaire poussiéreux ou écouter une heure de vidéo sur les bienfaits et le bien-fondé de la sécurité en entreprise n'apporte clairement rien à personne, si ce n'est une perte de

---

52 Cette norme qui a été publiée en 2005 pas l'*ISO* (*International Organization for Standardization*), ou *Organisation internationale de normalisation* (en français) est un document payant qui décrit les exigences pour la mise en place d'un *Système de Management de la Sécurité de l'Information* (*SMSI*). Ce document s'adresse à tous les types d'organismes (entreprises commerciales, administrations, ONG etc.).

53 La méthode de gestion des risques CORAS, est une méthode fondée sur des pictogrammes et avec un langage plus simple. Elle s'adapte facilement pour entrainer et sensibiliser des personnes dont la gestion du risque n'est pas le métier (ex : professions médicales, RH, utilisateurs finaux etc.). Ce premier lien : http://coras.sourceforge.net/documents/080828TheCORASMethod.pdf donne un aperçu des vignettes qui peuvent être utilisées. Le suivant : http://coras.sourceforge.net/documents/080828TheCORASMethod.pdf un exemple de scénario. Et le dernier : http://coras.sourceforge.net/index.html une description complète de la méthode pour le lecteur intéressé.

temps. Il faut peut-être à cet égard changer la culture d'entreprise et/ou modifier certains comportements. Ceci d'autant plus dans notre contexte, ou comme nous l'avons vu dans nos pages précédentes peu (pour ne pas dire quasiment pas) de mesures sont prises (rappelons peut-être à cet égard, que seulement 26% des sondés ont indiqué mettre sur pied un programme de sensibilisation prenant en compte ce risque [cf. sous-chapitre 2.2]). Les arguments invoqués sont souvent ceux du temps et de l'argent (le temps est précieux [le temps c'est de l'argent comme diraient certains] et des budgets suffisants ne sont pas forcément alloués pour ces aspects.) avec le peu de retour sur investissement immédiat que cela procure. Mais, il faut se poser la question de savoir si ce n'est pas pire comme risque de ne rien (ou peu) faire? Car bien souvent, une fois la survenue effective du risque (ici le *social engineering*), cela peut coûter bien plus que les éléments de prévention que nous aurions pu mettre en place initialement.

5.2 La sensibilisation à tous les niveaux

Les programmes de formation, prévention et sensibilisation doivent être adaptés au type d'activité de l'entreprise, au profil du personnel et à leurs tâches quotidiennes, voire au département :

> *« For awareness training to be effective it must focus on the employees real job, in real situation that they may encounter. »*[54]

Il n'existe pas une, mais plusieurs formules gagnantes. Suivant la culture d'entreprise, il sera plus judicieux d'adopter un scénario ou une approche plutôt qu'une autre. Dans tous les cas, quelle que soit la taille ou le secteur d'activité de l'entreprise, il est important que l'approche prenne en considération deux éléments majeurs :

1. Une dynamique *top down*, autrement dit *du haut vers le bas* de l'entreprise :

   «Les entreprises doivent maintenir leur personnel informé au sujet des différents types d'attaques dont une entreprise peut être victime, cela à tous les échelons de la hiérarchie. » (Gomez-Urbina, 2010, p.23)

   Tout le monde doit être concerné et sensibilisé au premier titre desquels la Direction. Ceci va permettre à la Direction des systèmes d'information (DSI), aux responsables de la sécurité, aux chefs de département, etc. d'avoir une assise solide dans leurs actions sur le terrain. Ainsi, tout le

54 La citation est tirée du document : *Engineering Capture the Flags Results – Defcon 19* écrit par *M. HADNAGY Christopher* en p.20. Le document peut être consulté à l'adresse suivante : http://www.social-engineer.org, via l'onglet CTF du menu principal en haut de la page d'accueil.

squelette hiérarchique marche d'un seul pas et donne une direction, un but et une dynamique d'ensemble pour l'entreprise.

2. Une dynamique *longitudinale* qui fait rentrer en ligne de compte les différents départements de l'entreprise, ses partenaires etc. Une entreprise quelle qu'elle soit ne peut se soustraire à son environnement. Elle opère à longueur de journée avec celui-ci pour gagner des nouveaux marchés, démarcher de nouveaux prospects, etc. De ce fait, il est important que les différents acteurs connaissent et appliquent les mêmes mesures. Les procédures doivent également être connues de tous. En effet, rien de plus facile pour un pirate de se faire passer pour un sous-traitant et porter une attaque. La sécurité n'est pas l'affaire d'une entité isolée, mais d'un ensemble d'acteurs agissant de concert.

Les RH, le Help desk, le standard et les utilisateurs finaux doivent faire partie de cette dynamique au même titre que le reste de l'entreprise et des partenaires. Bien souvent ils sont omis de ces programmes, généralement pour des questions d'économies.

> « *Most help desk employees are minimally educated in the area of security, so they tend to just answer questions and go on to the next phone call.* » (Megha et Sameer, 2012, p.31)

Il n'est pas rare (typiquement au Help desk ou au standard) qu'il y ait une forte rotation du personnel sur ces postes. Or, il ne peut y avoir une sécurité optimale si on ne prend pas en considération l'ensemble des acteurs de l'entreprise. C'est pourquoi, il est nécessaire de trouver un juste équilibre en la matière. De manière générale, toutes celles et ceux qui sont en contact direct et permanent avec l'extérieur doivent être sensibilisés à ce risque.

Dans ces programmes, il est aussi important d'aborder la notion d'information et l'importance qu'elle revêt dans la mitigation de ce risque. Le plus souvent par inadvertance ou ignorance, les employés qui de nos jours peuvent avoir leur propre blog, se montrent parfois indiscrets dans la publication de leur contenu. Il faut donner aux personnes les outils et les moyens de pouvoir détecter ce type de menace, mais il faut également mettre en place des procédures adéquates qui permettent d'y répondre.

5.3 Les moyens de mitigation

De manière plus spécifique, les contremesures et moyens de mitigation peuvent prendre place selon trois dimensions particulières que sont :

1. Les individus (le personnel)
2. Les processus et procédures
3. La technologie (les solutions techniques)

Les individus (le personnel) :

- Mettre des limites claires au personnel :
  L'ensemble des collaborateurs doit connaître les politiques de l'entreprise (politique des médias sociaux, de l'information, gestion des accès, etc.) avec les conséquences qui s'en suivent en cas de non-respect.

- Agir sur les tâches :
  Il s'agit de donner la possibilité technique et procédurale aux employés de vérifier l'information qu'ils ont le droit de divulguer lorsqu'une demande leur semble suspecte, de la contester le cas échéant.

- Etablir une vraie culture de l'information :
  Une pièce d'information, même en apparence anodine (exemple : numéro de téléphone) peut être utilisée pour mener une attaque. Les employés doivent prendre garde à ne pas transmettre plus de données que nécessaire et le cas échéant vérifier que la demande est légitime.

- Ne pas blâmer :
  Les cibles des ingénieurs sociaux sont des victimes. En punissant, blâmant ou stigmatisant ces personnes, ils seront moins enclin à admettre avoir (la plupart du temps à leur insu) donné des éléments qui ont probablement permis à l'attaque de se matérialiser. Or ces témoignages sont importants pour savoir qui a été ciblé, pourquoi et dans quelles circonstances. Ceci peut aussi permettre de tenir des statistiques (postes les plus à risque etc.) et évaluer la pertinence des outils mis en place.

Les processus et procédures :

- Feuilles de compte rendu d'incidents :
  Lorsqu'une activité suspecte (exemples : contact téléphonique avec personne suspecte, interaction directe au comptoir insistante, etc.) se manifeste, le personnel devrait remplir un formulaire qui détaille l'échange. Ce qui permet à l'entreprise de faire un premier tri et éventuellement d'ajuster ses mesures en conséquence si cela s'avère nécessaire.

- Notification des clients :

  Si un prospect ou un visiteur se voit refuser un accès, une information, etc., l'organisation peut rentrer en contact avec la personne à une date ultérieure pour l'informer des raisons du refus. Ceci peut également être utile pour vérifier si l'appelant a les droits souhaités (nécessaires) et faire un suivi des incidents.

- Itinéraire d'escalade :

  Il s'agit de mettre en place un processus d'escalade clairement défini, tout particulièrement pour le staff qui se trouve en première ligne. Des lignes hiérarchiques claires vont permettre de gérer l'incident rapidement et de capitaliser sur l'expérience. Par exemple, le collaborateur peut simplement rediriger l'individu suspect sur un manager plus expérimenté ou lui demander de faire parvenir sa demande par courriel : entreprise@info.com. Il évite ainsi d'être sous la pression directe d'un potentiel attaquant.

- Tester régulièrement :

  Vérifier à intervalle régulier l'efficacité et l'efficience des procédures, processus et outils déployés pour la mitigation du risque. Et plus particulièrement dans les zones sensibles ou plus susceptibles de faire l'objet de la menace.

La technologie (les outils techniques) :

- Sécurité physique :
  - Mettre en place des éléments de sécurité physique à l'entrée du bâtiment ou de certains départements jugés sensibles (carte d'accès & badges, scanners rétiniens, vigile, etc.). Toujours garder à l'esprit qu'il ne faut pas miser tout sur cet aspect uniquement, mais qu'il fait partie d'un ensemble de mesures pour contenir le risque.

- Sécurité logicielle :
  - Les patchs de sécurité, les anti-virus, pare-feu et autres filtres anti-spam doivent être installés, testés et mis à jour régulièrement.
  - Pour les pare-feu, le principe de l'oignon devrait être appliqué (c'est-à-dire plusieurs couches de protection. Par exemple : un pare-feu à l'entrée du réseau d'entreprise, un autre sur le sous-réseau et une protection sur la machine de l'utilisateur final.)

- Les dernières mises à jours des logiciels doivent être installées aussitôt que possible sur les postes.

- Sécurité technique :
  - L'installation de système de prévention et/ou détection d'intrusion.
  - La mise en place d'une DMZ.
  - Tout autre élément de sécurité jugé pertinent et utile en fonction des besoins de l'entreprise (exemple : enregistreur d'appels téléphoniques).

5.4 Tests d'intrusion et audits

En plus de tout ce que nous avons discuté jusqu'ici, les tests d'intrusion et les audits sont des outils importants qui vont permettre à un professionnel de la sécurité dûment mandaté[55] par l'entreprise de vérifier, évaluer et tester les éléments suivants :

- La formation du personnel
- Les politiques mises en place
- Les processus et procédures
- Les éléments de sécurité physique et technique

L'objectif principal des tests d'intrusion c'est d'évaluer dans le cadre de l'audit, quelle est la résistance (la force) du maillon humain de la sécurité du système d'information, de la même façon qu'une entreprise mène des audits pour traquer et dépister de nouvelles vulnérabilités de son système informatique. Comme l'illustre la figure ci-dessous, l'aspect humain est une chaîne primordiale, qui est malheureusement bien souvent occultée en axant les mesures de sécurité la plupart du temps uniquement sur les dimensions physiques et techniques. Or, une chaîne n'est jamais aussi forte que son maillon le plus faible.

55 De façon générale ce type de mandat est confié à une structure externe avec des auditeurs spécialisés dans l'évaluation de la sécurité du système d'information. Dans les grandes compagnies, il peut toutefois y avoir un service interne d'audit.

Figure 9 - Human security – the missing link. Le schéma est directement adapté de la source qui suit. Source : Mann, Ian : *Hacking the Human : Social Engineering Techniques and Security Countermeasures*. Gower. Burlington (USA) : 2008, p.2

Comme nous pouvons l'apercevoir ci-dessus, le lien humain est capital dans la prévention du risque et tout particulièrement dans notre contexte.

Il est nécessaire que l'auditeur et le client commencent par se mettre d'accord sur le(s) but(s) et les objectifs à atteindre. Ceci constituera une base commune de discussion qui permettra au client à l'issue de l'évaluation de mieux appréhender l'importance de certaines failles, de prendre d'éventuelles nouvelles dispositions en matière de sécurité et d'affiner, corriger les programmes de sensibilisation et de formation en conséquence. Chacun de ces buts est ensuite priorisé en fonction de l'importance qu'il revêt pour l'entreprise (en tenant compte de son secteur d'activité, les mesures de sécurité déjà présentes ou encore si l'entreprise est rompue ou non à ce type d'exercice). L'évaluation des buts peut être déterminée à partir d'une échelle d'importance du type 0 à 10 (0 : aucune importance ; 10 : prioritaire). Un autre avantage de ce système de fixation des buts est qu'il permet de vulgariser certains aspects souvent très techniques de la sécurité à des personnes dont le cœur de métier n'est précisément pas celui-ci. Un exemple de liste de buts est donné ici :

- *To determine whether employees will click on links in emails or open files from people they do not know well, leading to compromise*
- *To determine whether an employee would go to a website and enter personal or business-related information on that site*

- *To determine how much information can be obtained via the phone or in-person visits of employees at work or personal places (that is, bars, gyms, daycares)*
- *To determine the level of security in the office perimeter by testing locks, cameras, motion sensors, and security guards*
- *To determine the ability of a social engineer to create a malicious USB or DVD that will entice the employee to use it on his or her work computer, compromising the busines*[56]

Certains objectifs peuvent aussi comporter des parties où il s'agit de gagner l'accès à des zones sensibles du bâtiment ou encore la possibilité d'obtenir une information particulière (si possible confidentielle) :

- *Get into the data server room*
- *Obtain information from the CEO's office*
- *Get a sample of your confidential designs*[57]

Les listes ci-dessus ne sont pas exhaustives, mais encore une fois, il est important que ces buts puissent être en relation avec les besoins de l'entité. Une fois cette première partie clairement déterminée, l'audit peut alors prendre corps et la phase de test est initiée. Ceci se fait généralement sous la forme de quatre étapes distinctes :

1. La récolte des informations sur l'entreprise et son environnement ainsi que sur les employées. L'expert opère généralement de la même manière qu'un ingénieur social : visite du site corporatif et/ou celui des partenaires, sous-traitants, récupération de documents via le Web etc. Cette première étape va permettre de repérer et lister les vulnérabilités. Ce qui sera utile pour la constitution du rapport final, le feed-back au client et le passage à l'étape suivante.
2. À partir des vulnérabilités identifiées s'opère le choix de la cible pour le futur test de pénétration. On sélectionne le meilleur vecteur d'attaque autour duquel on construit un scénario.
3. Le test de pénétration est exécuté sur le terrain en exploitant la cible. Le déroulement du test et sa sortie (échec ou réussite) seront notés.
4. Constitution d'un rapport et feed-back au client.

---

56 Les éléments sont tirés du livre :

- HADNAGY, Christopher. *Social Engineering : The Art of Human Hacking*. Wiley Publishing, Inc. Indianapolis, Indiana : 2011. p.350

57 Les éléments sont tirés du livre :

- MANN, Ian. *Hacking The Human : Social Engineering Techniques and Security Countermeasures*. Gower. Burlington (USA) : 2008, p.221

Les tests d'intrusion se matérialisent sous la forme d'un scénario, d'un prétexte que l'auditeur met directement en action sur le terrain. Afin d'imager cet aspect de la procédure, voici deux brefs exemples donnés par des experts du domaine :

> *« In one audit the pretext I used was being the assistant to the CFO[58]. The call center employees had a fear of losing their jobs for rejecting the requests from such a high-level management. Why? They are not given the proper education to know that rejecting that request would not cost them their jobs. At the same time protocols should be in place for the employee to know when a request for information is proper. »*[59]

> *« Assuming the identity of an auditor is a great way to gain access to information. Many people are effectively conditioned to allow anyone claiming to be an auditor to access any information, and often to take copies at wil. »*[60]

Les tests d'intrusion et les audits réguliers vont permettre :

- Une évaluation régulière de l'apport des employés dans le dispositif de mitigation au *social engineering.*
- De savoir où se situe l'entreprise : quels sont les progrès effectués et ceux à planifier pour le futur.
- Consolider la création d'une réelle culture d'entreprise vis-à-vis de ce risque, avec une prise de conscience accrue et une participation des cadres dirigeants.

Il est primordial que l'entreprise puisse aussi capitaliser sur l'expérience de ces exercices pour améliorer ses processus et la prise de conscience du personnel. Un moyen concret, efficace et immédiat pour elle de profiter de ce feed-back, peut simplement consister à mettre en place des scénarios, des scripts qui permettront (sur la base du vécu) aux employés de savoir quoi répondre et comment se comporter dans les situations problématiques rencontrées. Un parfait exemple est donné par M. HADNAGY[61] :

---

58 En anglais, *CFO* signifie Chief financial officier (ou : Directeur financier en français)

59 Exemple tiré du livre :

- HADNAGY, Christopher. *Social Engineering : The Art of Human Hacking*. Wiley Publishing, Inc. Indianapolis, Indiana : 2011. p.345

60 Exemple tiré du livre :

- MANN, Ian. *Hacking The Human : Social Engineering Techniques and Security Countermeasures*. Gower. Burlington (USA) : 2008, p.16

61 Exemple tiré du livre :

- HADNAGY, Christopher. *Social Engineering : The Art of Human Hacking*. Wiley Publishing, Inc. Indianapolis, Indiana : 2011. p.348

« Scripts can help an employee determine the proper response during these circumstances and help them feel ease. For example, a script may look like this : If someone calls and claims to be from the management office and demands compliance of either handing over information or internal data, follow these steps :

1. *Ask for the person's employee ID number and name. Do not answer any questions until you have this information*

2. *After getting the identifying information, ask for the project ID number related to the project he or she is managing that requires this information*

3. *If the information in steps 1 and 2 is successfully obtained, comply. If it's not, ask the person to have his or her manager send an email to your manager requesting authorization and termine the call*

A simple script like this can help employees know what to say and do in circumstances that can try their security consciousnes. »[62]

Les audits et les tests d'intrusion doivent être correctement menés (ne pas blâmer ceux qui se sont fait avoir, respecter les règles éthiques en la matière, etc.) et des limites claires doivent être posées pour éviter tous problèmes ultérieurs (fuite ou accès à des informations non-voulues, etc.). Il peut aussi être important d'inclure dans le processus d'audit un ou plusieurs membres de l'entreprise. Et plus particulièrement du personnel des équipes de sécurité, de la direction des systèmes d'information et si possible un membre de la direction. Ils garantissent ainsi que les éléments sensibles révélés par les tests restent dans le périmètre de l'entreprise. Et enfin, en participant au processus d'évaluation, le sentiment éventuel de remise en cause des éléments de sécurité mis en place (lié au fait que l'audit s'effectue généralement par une personne extérieure. Ce qui peut générer un sentiment d'intrusion, de fouille) est atténué au profit d'une plus grande focalisation sur le retour d'expérience.

Remarques :

Pour le lecteur qui souhaite aller plus loin dans la compréhension ou la mise en pratique des audits de sécurité, nous conseillons les deux ouvrages suivants :

- *Hadnagy, Christopher : The art of Human Hacking*
- *Mann, Ian : Hacking the Human – Social Engineering techniques and Security Countermeasures*

Le premier ouvrage permet une approche de l'audit plus simple et s'adressant à un public plus large. Quant au deuxième, il se révèle plus technique et s'adresse à un public de professionnels de la sécurité avec une mise en application possible. Les références complètes sont données dans notre bibliographie.

62 Le livre *The art of deception de D. Mitnick, Kevin et L. Simon, William* offre la possibilité d'avoir toute une série de scénarios déjà pré à l'emploi avec des schémas d'action définis en pp.331-338 (cf. la bibliographie).

6. L'entreprise moderne comme catalyseur

6.1 La gestion de l'information

Il est tout à fait normal que dans un contexte d'entreprise, l'échange, le partage et la publication de contenu soit monnaie courante[63]. Que ce soit pour communiquer sur ses produits, faire de la promotion et du marketing, trouver de nouveaux partenariats ou encore mandater un tiers pour un projet, les actifs informationnels sont au cœur des activités métiers d'un business. Cependant, bien qu'il semble logique et acquis de fait dans tous les esprits, qu'il faut protéger ses brevets et autres données jugées sensibles sur des supports hyper sécurisés (à priori car, comme nous le montrerons par la suite, on peut se poser de sérieuses questions), l'information au sens large du terme, ne jouit elle que d'une faible attention de la part du management et des équipes de sécurité. La figure ci-dessous illustre parfaitement le problème de la fuite et de l'importance de correctement encadrer la gestion de l'information pour une entreprise, avec toutes les conséquences que cela peut représenter :

63 Bien évidemment ces éléments ne sont pas propres au domaine de l'entrepreneuriat, mais à toutes les activités humaines en générale.

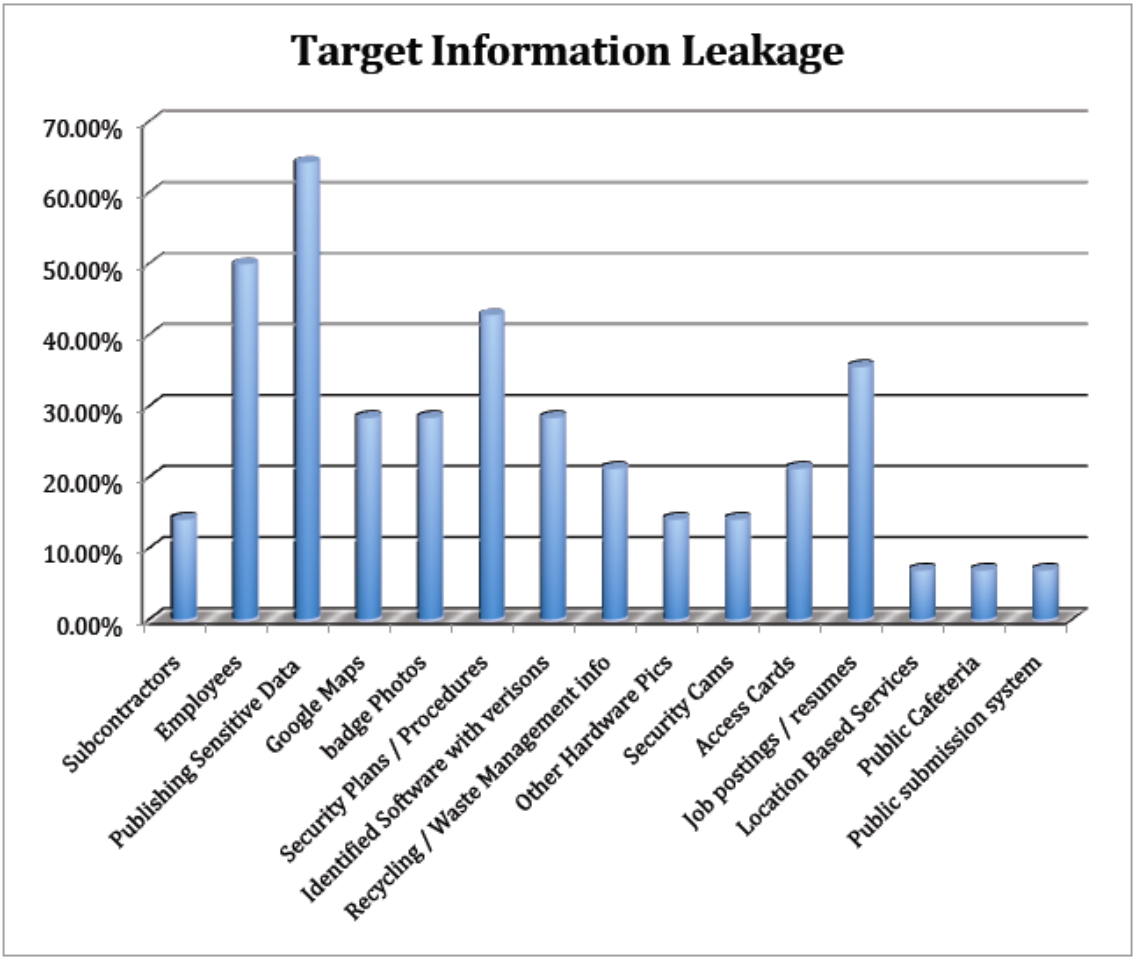


Figure 10 – La fuite d'information dans le domaine publique en entreprise. Cette image permet d'illustrer le problème de la fuite de diverses sources d'informations d'entreprise dans le domaine public. Les entreprises qui ont été testées au cours de cette édition du DEFCON (ici DEFCON-19) étaient au nombre de quatorze : *Apple, AT&T, Conagra Foods, Dell, Delta Airlines, IBM, McDonalds, Oracle, Symantec, Sysco Foods, Target, United Airlines, Verizon et Walmart.* Pour chaque source de données, il est inscrit le pourcentage d'entreprises l'ayant laissé filtrer publiquement. Par exemple : 70% d'entre elles ont laissé passé des données dites sensibles et un peu plus de 40% ont publiées des éléments concernant les procédures et plans de sécurité etc. Précisons encore que tous ces éléments on été recueillis par des outils disponible de tous (moteurs de recherche etc.). Source : HADNAGY Christopher : *Social Engineering Capture the Flags Results – Defcon 19*. 2011, p. 16

Le constat que l'auteur fait est alors sans appel :

« With close to 70% of the companies leaking some form of sensitive data, it is not too harsh to say that full-scale social engineering attacks could be launched with little more than the passive information that was gathered by the social engineers. »[64]

À la simple vue de ces résultats, nous sommes en droit de nous poser la question de savoir, si raisonnablement des mesures sont prises pour réellement sécuriser et gérer

64 La citation est tirée du document : *Engineering Capture the Flags Results – Defcon 19* écrit par *M. HADNAGY Christopher* en p.16. Le document peut être consulté à l'adresse suivante : http://www.social-engineer.org, via l'onglet CTF du menu principal en haut de la page d'accueil.

convenablement certaines sources d'informations? Que certaines données se retrouvent publiées pour tous cela nous paraît logique. Nous pensons notamment ici aux grandes compagnies d'aviation (*Delta et United Airlines*) ou encore aux opérateurs de téléphonie mobile et fournisseur d'accès internet (*AT&T et Verizon*), qui de par leurs activités doivent communiquer vers l'extérieur (service de conseil et d'aide à la clientèle etc.). Mais comment justifier que l'on puisse trouver des informations concernant les cartes d'accès, les procédures de sécurité, les logiciels employés et leurs versions etc. Imaginez un seul instant les dégâts que cela pourrait causer : crash d'un avion par le piratage d'un logiciel embarqué à distance, couper les communications d'une ville ou d'une région, piratage de réseau télécom etc.

On comprend dès lors beaucoup mieux de quelle façon l'entreprise contemporaine est un catalyseur de ce risque, en étant pour grande partie elle-même la source privilégiée, la plateforme de lancement des attaques qui lui sont destinées. Une surveillance régulière et accrue des informations sur l'organisation flottant sur le Web en particulier, est devenue une nécessité. Tout type d'irrégularité doit être immédiatement pris en charge et rendra ainsi la collecte d'informations passive beaucoup plus difficile pour l'attaquant. Les comportements et les mentalités doivent changer et ceci passe notamment par le création d'une réelle culture d'entreprise sur la valeur de l'information. Quelle que soit la taille, l'importance ou le volume de la pièce d'information, cette dernière peut revêtir une importance capitale pour la sécurité de l'entité. Certaines règles de bons sens devraient également être appliquées à cet égard :

1. L'utilisation d'identifiants propre à l'entreprise dans le domaine public (blogs, forums de discussion etc.) doit être fortement limité.
2. Ne pas afficher des informations compromettantes sur son site ou tout autre plateforme (entre autres les sites des partenaires commerciaux, sponsors etc.), qui n'est pas digne de confiance.
3. Ne pas divulguer de renseignements personnels ou des informations sur notre organisation, sauf si nous en avons reçu l'autorisation ou que le tiers est digne de confiance.
4. *« Prudence est mère de sûreté »*. Éviter alors autant que posible d'afficher des tableaux, données financières, listes des projets importants ou listes des personnes clés de l'organisation.
5. Éviter de donner des informations sur les services utilisés et leur version.
6. De manière générale, toute information qui pourrait potentiellement donner la possibilité à un attaquant d'exploiter une faille quelconque, doit être bannie des supports publics de l'entreprise.

Tout comme la formation et la sensibilisation, la gestion de l'information est un élément clé du dispositif de mitigation. Le volume d'information ne cesse de croître et il y a fort à parier que son importance ira grandissante. Il suffit de voir les technologies et outils qui se sont développées et continuent à se développer ces dernières années : les systèmes Big Data, les data warehouse, l'OLAP ou encore le data mining (cf. glossaire p.85 pour les définitions des termes), ne sont que quelques exemples parmi d'autres. Pour toute une série d'industries, les enjeux liés à l'information sont colossaux. L'information et tout particulièrement le système d'information d'une entreprise représente sa vraie valeur. Le protéger et éduquer les personnes à cet égard est essentiel car, le compromettre c'est aussi mettre en danger toute l'entité.

Pour aider à cette gestion, il devrait y avoir en entreprise une classification correcte et claire des données sur la base de leur niveau de criticité et du personnel qui peut y avoir accès.

6.1.1 Les débuts d'une politique de l'information

Une piste possible pour gérer son actif informationnel au mieux, est clairement celle de l'élaboration et la mise en œuvre judicieuse d'une politique de l'information. Le but de nos lignes ici n'est pas de développer au complet le squelette général de ce que devrait être une bonne politique en la matière. Chaque entité jugera en fonction de ses besoins (présent et futurs), de ce qu'elle a déjà mis en place (ou non) et de la forme et du contenu de ses documents. Nous proposons ici deux modèles de classement de l'information, deux moyens de mitigation (contre-mesures), qui nous semblent intéressant d'inclure (ou en tout cas de considérer) pour aider à minimiser le risque de fuite d'information. Ces modèles sont ensuite mis en relation avec une classification des personnes pour constituer ce que nous appelons une matrice de sensibilité. Ces trois éléments (modèle de classement de l'information, modèle de classement des personnes et la résultante qui est une matrice de sensibilité) devraient figurer dans la politique.

La classification de l'information :

Le classement de toutes les informations de l'entreprise est une démarche qui :

- Demande du temps.
- Nécessite une vision stratégique d'ensemble, la collaboration des divers départements, de la Direction des systèmes d'information et des équipes de sécurité.
- La création d'une équipe dédiée pour porter le projet à son terme et faire le suivi. Ceci peut alors nécessiter des moyens humains importants

La classification des données va permettre d'assigner un niveau de sensibilité à l'information de l'entreprise. Chaque niveau de classification de données inclut des règles différentes pour la visualisation, l'édition et le partage des données. Ainsi, elle aide à prévenir l'ingénierie sociale en offrant aux employés un mécanisme pour comprendre ce qui peut être divulgué et ce qui ne peut pas être partagé sans autorisation. Une fois la classification effectuée, les informations doivent être revues régulièrement (déclasser, reclasser [réévaluer] etc.), plus particulièrement celles considérées comme stratégiques pour l'entreprise. Ceci garantit la mise à jour des droits correspondants, la robustesse du système et sa pérennité.

- **La classification par genre :**

  Ce système catégorise les informations en fonction du type de la donnée :

  - ***informations financières :***

    Données relatives au flux financier de l'entreprise (bénéfices, pertes, investissement etc.).

  - ***informations techniques :***

    Données relatives aux brevets, savoir-faire ou des projets en développement.

  - ***informations juridiques :***

    Données concernant le cadre légal et juridique.

  - etc.

  Le nombre de catégories (c'est-à-dire la granularité du classement) dépendra des données de l'entité et de ses besoins.

- **La classification par niveau :**

  Ce système catégorise les informations en fonction du niveau de confidentialité (d'importance) de la donnée :

  - ***Informations publiques :***

    Toutes les informations que ne mettent pas en danger l'entreprise, ses clients, ses partenaires commerciaux.

- ***informations internes :***

  Toutes les informations qui sont produites, utilisées et distribuées dans les murs (le cadre) de l'entreprise

- ***informations privées :***

  Les informations spécifiques à un département

- ***informations sensibles :***

  Les informations restreintes à un tout petit groupe de collaborateurs ou un individu

Encore une fois, d'autres alternatives sont possibles : *public*, *privé*, *restreint* et *secret* par exemple.

La classification des personnes :

Le classement du personnel dans des groupes va permettre de définir les aspects suivants :

- Qui a le droit d'accéder à quoi?
- Quand?
- Dans quelles circonstances?
- Et selon quel mode de partage?

La répartition du personnel peut s'effectuer en fonction :

- De ses accès & accréditations
- Du profil (élevé, moyen ou faible)
- Du poste (manager, chef de département etc.)
- De l'ancienneté

L'entreprise choisira ensuite quels sont les groupes les plus adaptés en fonction de ses attentes et besoins. À noter qu'il ne s'agit pas d'un système figé, mais qui doit suivre le développement de l'entreprise. Au final, c'est l'entrecroisement des niveaux de classification des informations avec ceux du personnel qui va permettre de visualiser et définir quel groupe a accès à quelles informations. Il est alors fondamental que ce document puisse être distribué à tous les collaborateurs. En cas de doute, les personnes de l'entreprise pourront ainsi s'y référer.

De plus, dans le cadre de son élaboration, la politique de l'information doit également prendre en compte dans son périmètre d'action les tierces-parties avec qui l'entreprise collabore. Ce document doit être connu et appliqué adéquatement par les sous-traitants, partenaires commerciaux etc. Elle indiquera de la même manière qu'avec ses propres employés, les informations auxquelles ils ont accès et les modes de partage autorisés.

En plus de la politique, il peut être nécessaire (voir obligatoire selon les législations, les secteurs d'activité, etc.) de faire signer un document de non-divulgation (confidentialité). Ces deux éléments combinés garantissent une assise solide à la protection des données d'entreprise et indiquent les pénalités en cas de non-respect.

L'information est une pièce maîtresse pour un ingénieur social. Sans cette dernière, il lui est impossible de construire le bon scénario et de donner corps à son attaque. Nous comprenons dès lors l'importance de correctement protéger ses données. Alors qu'une politique de sécurité globale d'entreprise va essentiellement axer ses moyens de mitigation sur des aspects techniques et sur la qualité des supports contenant les données, elle n'intervient que très peu sur les modes de partage, l'accès aux données ou le profil des personnes y accédant. En ce sens, la politique de l'information est un document nécessaire et fondamental qui vient consolider la politique en matière de sécurité d'une entreprise. De la même façon qu'un responsable de la sécurité va porter une attention particulière à l'architecture de son réseau, à choisir le bon matériel (solidité, robustesse face à certains types d'attaques etc.) et installer les logiciels de protection adéquats, l'information devrait elle aussi bénéficier de tous ces égards. Dans un monde ou la guerre de l'information ne fait que commencer et où celle-ci est devenu un acteur économique prépondérant, nous pouvons croire que le développement et l'impact de ce risque ira grandissant. La politique de l'information est un outil d'une portée essentiel dans le contexte sécuritaire de l'entreprise de demain[65].

65 Si le lecteur souhaite aller plus loin dans ce sujet ou avoir des compléments d'informations sur les politiques qui peuvent lui servir dans ce contexte, nous lui suggérons alors de consulter l'ouvrage suivant : *The art of deception de D. Mitnick, Kevin et L. Simon, William, chapitre n°16*. (cf. bibliographie pour les détails)

6.2 Social engineering et politique de sécurité

Le cadre *ISO 27001* est le standard sur lequel se base la grande majorité des entreprises pour la mise en place d'un *SMSI*[66]. Il dessine les contours et donne les grandes lignes directrices et recommandations pour constituer :

- Une politique de sécurité
- Une ébauche de gestion de l'information
- La gestion de la sécurité physique et environnementale
- La sécurité des équipements
- Ou encore les bonnes règles pour les back-ups
- Etc.

Tout ceci est dûment décrit dans le document et prend la forme d'une liste de 133 mesures de contrôle qu'il est possible d'implémenter en fonctions du domaine à sécuriser. Malgré cela, il n'apporte aucun élément concret dans le traitement ou la mitigation du risque d'ingénierie sociale :

> *« One weakness of the current ISO 27001 standard is that, although in many ways it is broad in is coverage of security, its recognition of social engineering is poor. With only minimal coverage on user awareness and training, it fails to direct people to a fuller understanding of social engineering threats. »*
>
> *(Mann, 2008, p.15)*

Cependant, malgré ce que certaines personnes peuvent penser, ce standard n'est de loin pas une liste exhaustive de tous les risques informatiques existants et ne répertorie de loin pas l'ensemble des contremesures qu'une entreprise peut ou doit mettre en place. Il ne s'agit là que de recommandations. D'ailleurs, si nous examinons de plus prêt sa clause *4.2.1 g)*, voici ce qu'il est possible d'y lire :

> *« The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.*
>
> *NOTE: Annex A contains a comprehensive list of control objectives and controls that have been found to be commonly relevant in organizations. Users of this International Standard are directed to Annex A as a starting point for control selection to ensure that no important control options are overlooked. »*[67]

---

66 SMSI pour : *Système de Management de la Sécurité de l'Information*. Ce référentiel est utilisé par tout type d'industries. Il existe d'autres référentiels pour implémenter un SMSI comme par exemple : *ITIL Security Management ou COBIT.*

67 Extrait directement tiré depuis la norme elle-même (cf. bibliographie sous norme).

Ainsi, il est non seulement possible, mais utile et recommandable de compléter sa propre politique de sécurité interne avec le risque que nous traitons ici et les moyens de mitigation adéquats. L'entreprise en sortira renforcée en ayant une meilleure représentation (plus complète, plus construite) des risques pesant sur ses activités, car rappelons-le, il reste encore du chemin à parcourir à cet égard :

> *« Due to lack of attention paid to this threat, there is no indication that this situation will change soon »*[68]

68 La citation est tirée du document : *Engineering Capture the Flags Results – Defcon 19* écrit par *M. HADNAGY Christopher* en p.16. Le document peut être consulté à l'adresse suivante : http://www.social-engineer.org, via l'onglet CTF du menu principal en haut de la page d'accueil.

7. Conclusion

7.1 Synthèse du travail de recherche

De manière générale, le maître mot que nous retenons ici c'est : *éduquer*.

- Éduquer pour les médias sociaux
- Éduquer pour les biais
- Éduquer pour l'importance de l'information
- Éduquer sur le risque lui-même

Éduquer pour les médias sociaux :

Alors que les nouvelles technologies de l'information et de la communication ont littéralement envahi nos vies, il est effarent de constater à quel point ces dernières sont si peu considérées dans la gestion de la sécurité en entreprise de manière générale. Les consciences doivent évoluer dans ce sens notamment quant à la sensibilisation à ces nouveaux outils. Contrairement à ce que l'on pourrait penser de prime à bord, leur utilisation n'est pas anodine. Rappelons-ici qu'ils sont concernés au premier chef en matière de fuite d'information. Protéger et encadre l'usager, c'est également assurer la sécurité de son entreprise.

Éduquer pour les biais :

L'ingénierie sociale, c'est le risque de l'humain en tant qu'il est. C'est-à-dire dans ce qu'il est de plus simple. Si vous voulez sensibiliser et former votre personnel, dans la perspective d'en faire une première ligne de défense solide pour la mitigation à ce risque, vous devez lui apprendre à connaître et reconnaître les failles humaines. Seulement ainsi il apprendra à détecter et contrecarrer la menace pour garantir une sécurité optimale.

Éduquer pour l'importance de l'information :

Tous les jours nous échangeons, modifions, éditons quantité de données et ce avec une certaine banalité. Une politique de l'information permet de contrôler, organiser et structurer les flux informationnels de l'entreprise. L'existence d'une telle politique prive l'ingénieur social de la substance première qu'il recherche.

Éduquer sur le risque lui-même:

Le risque lui-même est peu connu. On communique peu sur ce dernier et lorsqu'il arrive aux oreilles des responsables de la sécurité, il est très souvent sous-estimé (parce que ce n'est pas un risque technique). Quant aux employés eux-mêmes, qui sont bien souvent démunis face à ce problème, on leur demande d'être attentifs et de

protéger au mieux les actifs de l'entreprise. Dans ces circonstances quelque peu paradoxales, un constat s'impose : il est nécessaire d'éduquer et sensibiliser le personnel dans son ensemble. Les responsables de la sécurité doivent se rendre compte que l'on est en train d'attaquer leur meilleur atout dans la mitigation de ce risque : leurs collaborateurs. De l'autre côté, il faut donner des outils à ces mêmes personnes pour agir et non pas subir. Enfin, une mobilisation de la Direction est aussi nécessaire pour donner une ligne directrice, un cap.

Comme nous l'avons décrit tout au long de nos pages, il n'existe malheureusement pas une mesure de mitigation unique et efficace qui permette aujourd'hui de se prémunir efficacement de ce risque. Par ailleurs, le principal standard en la matière, ne propose guère plus que quelques recommandations. Et ceci n'est pas prêt de changer dans l'immédiat. À la lecture de ce constat plutôt accablant, nous serions en droit de nous dire : que faire?, par où commencer?, comment?, quand? La bonne nouvelle c'est qu'il y a justement tout (ou presque) à construire, innover et imaginer. L'immobilisme n'est pas une solution, mais un signe de fatalité. C'est au dirigeant de demain et à ceux d'aujourd'hui de lancer l'initiative, mettre le moteur en route. Nous pourrions simplement commencer par ces quelques étapes :

- Former, éduquer et sensibiliser le personnel en lui apprenant à reconnaitre le risque
- Établir une réelle culture de l'information et également un sens commun de la sécurité : *La sécurité est l'affaire de tous*
- Rendre attentif à l'usage des nouvelles technologies et de leur(s) impact(s)
- Mettre en place des audits et des tests d'intrusion spécifiques
- Changer les mœurs et faire évoluer les consciences

7.2 Un apport personnel

Dans le cadre de notre formation à la fois de technicien et de gestionnaire, nous avons appris à segmenter un réseau, à correctement sécuriser machine personnelle et un serveur dédié ou encore à évaluer, rapporter et mitiger les principaux risques informatiques. Mais voilà, rien de bien probant sur le thème traité dans ce travail. Si ce n'est une courte intervention d'une dizaine de minutes par un auditeur, dans le cadre d'un cours de gouvernance du système d'information (SI) il y a maintenant deux ans. Or, étant de nature curieuse et nous intéressant particulièrement au management et à la sécurité du SI, nous nous sommes donc tout naturellement petit à petit mis à regarder dans cette direction. Le travail de Bachelor était alors pour nous l'occasion parfaite d'approfondir nos connaissances sur ce risque et surtout de le faire connaître.

Notre ambition ici est celle de présenter et de mettre en lumière par notre travail cette menace peu connue et peu prise en considération. Nous avons notamment appris à connaître ses contours et ses particularités qui font de ce risque un élément complètement à part de ce que nous avions pu aborder jusqu'à lors. Nous en avons également appris beaucoup plus sur la complexité du système d'information et de ses mécanismes au gré de mes diverses lectures. Nous espérons modestement ainsi donner des solutions concrètes (ou piste d'idées) à ceux qui s'intéressent aux risques en général.

Pour arriver au dossier que nous présentons ici, il nous a fallu persévérer, creuser et chercher en profondeur les informations nécessaires à notre devoir scientifique. La littérature spécialisée ne commençant que récemment à s'intéresser à ce phénomène, les ouvrages traitant du problème ne sont pas légion, et encore moins lorsqu'il s'agit de l'associer à des mesures de sécurité concrète. La plupart des rapports ou articles dépeignent les contours, apportent quelques détails sur les techniques, sur les ruses employés, mais rien de bien probant. Ce qui montre d'ailleurs que beaucoup de choses restent encore à faire dans ce domaine. Grâce à cette recherche approfondie, nous avons pu découvrir de nouvelles, précieuses et enrichissantes sources d'informations. C'est également là quelque chose que nous souhaitons partager avec le lecteur qui souhaite aller plus loin dans sa compréhension ou qui veut mettre en place des éléments de sécurité dans son entreprise.

Enfin n'oublions pas, que la sécurité du système d'information par l'humain pour l'humain est une aventure complexe et enrichissante qui nous demande d'ouvrir de nouveaux horizons et trouver de nouvelles possibilités :

> *« Humans are much more complex, less understood and present a bigger challenge in addressing security vulnerabilities. » (Mann, 2008, p.21)*

Glossaire

API :

Une *API* pour *Application Interface Programming* (en anglais), ou interface de programmation (en français), est un ensemble de classes, de méthodes et de fonctions qui permettent à un logiciel (logiciel fournisseur) des fonctionnalité(s) à un ou plusieurs logiciels (logiciel consommateur). Le concepteur de bibliothèque (concepteur de l'API) fournit une documentation sur sa conception, spécifiant ses fonctionnalités et son utilisation.

Big Data :

Le *Big Data* ou littéralement les *Grosses (Grandes) données* (en français), est un terme qui fait référence à des ensembles de données très volumineux. À tel point qu'il devient difficile de traiter ces volumes d'informations avec des outils classiques de gestions de base de données ou de gestion de l'information. Ces gros volumes sont produits par tout type d'industrie (pharmaceutique, aérospatiale, etc.). L'analyse de ces données pourrait par exemple permettre de prédire une épidémie, une sécheresse, de faire des projections de ventes plus fines, etc.

Cryptographie :

La cryptographie est la discipline qui s'attache à protéger des messages en se basant sur des *clés.* Les clés pouvant être *publiques* ou privées et permettent ainsi l'échange d'informations sécurisées entre un émetteur et un récepteur.

Data mining:

Le *data mining*, ou *fouille de données* (en français) est une discipline au croisement de l'informatique, les mathématiques et les sciences sociales qui a pour but d'extraire un savoir, des connaissances à partir de grandes quantités de données. Ceci s'effectue généralement par des outils informatiques automatiques ou semi-automatiques.

Data warehouse:

Un *data warehouse, ou entrepôt de données* (en français) est un terme qui se rapporte à une base de données de très grande capacité pour collecter, ordonner, journaliser et stocker des informations provenant des base de données opérationnelles de l'entreprise et/ou de ses partenaires commerciaux. Ces données sont généralement utilisées comme outil d'aide à la décision (connaître les opinions des consommateurs, campagne de marketing ciblée, etc.).

Défacement :

Le *défacement*, *défaçage*, *falsification* ou *défiguration de site web* est une technique de piratage qui consiste à détourner tout ou partie d'un site Web. La plupart du temps, il s'agit de la page d'accueil ou d'une page contenant des formulaires clients et appartenant à des entreprises, institutions connues du public. Il est ainsi plus facile de baisser la vigilance de la cible et lui soutirer les informations voulues (en lui pressant de bien vouloir fournir telles ou telles informations sous le couvert d'un prétexte quelconque). Elle n'est pas une technique à proprement parler en soi, mais est très utilisé avec le *phishing*.

Firewall :

Un *firewall*, ou *pare-feu* (en français) est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, en définissant quelles sont les communications autorisées sur ce réseau. Il existe différentes catégories de pare-feu : applicatif, à états (*stateful firewall*), sans état (*stateless firewall*) etc.

Keylogger :

Un *keylogger*, ou *enregistreur de frappe* (en français) est le plus souvent un logiciel espion (mais peut aussi se présenter sous la forme d'un périphérique), qui espionne électroniquement l'usager d'un ordinateur. Ses buts sont variés, mais il permet de récupérer mots de passe, codes d'accès, noms d'utilisateur, etc. En gros tout ce qui est frappé sur le clavier par l'utilisateur. Certains sont capables de faire preuve de fonctionnalités avancées en récupérant fichiers, captures d'écran, etc. sur le réseau de la personne pour les transmettre à distance.

Logiciel antivirus :

Un *logiciel antivirus* est un logiciel conçu pour identifier, neutraliser et éliminer d'éventuels logiciels malveillants (malwares). Les virus ne constituant qu'une catégorie possible, mais nous pourrions citer les chevaux de Troie, les vers informatiques etc.

OLAP:

L'OLAP (*OnLine Analytic Processing)*, ou *traitement analytique en ligne* (en français), est généralement un type d'application informatique qui permet l'analyse en temps réel d'informations selon plusieurs dimensions possibles. Le but étant d'avoir une vue particulière sur une activité, ou de zoomer sur des informations spécifiques au milieu d'autres données pour en ressortir les éléments intéressants pour l'entreprise. À noter qu'il existe plusieurs types d'OLAP et qu'ils sont généralement employés comme outil d'aide à la décision.

Outsourcer :

Le mot outsourcer, ou externalisation (en français) signifie le transfert complet ou partiel d'une ou plusieurs activités (généralement des activités périphériques, qui ne sont pas considérées comme le cœur de métier) d'une entreprise ou d'une administration vers un partenaire externe. On parle alors volontiers de sous-traitance. Celle-ci peut s'effectuer dans le même pays, sur le même continent ou dans d'autres pays du globe. Les deux parties sont généralement tenues par un contrat, qui stipule les conditions de l'accord. Tout ou presque peut faire l'objet d'une sous-traitance : développement informatique, les ressources humaines, la sécurité informatique etc.

Phising :

Le *phishing*, ou *hameçonnage* (en français) est une technique qui consiste à faire croire à l'usager qu'il s'adresse à un tiers de confiance (banque, administration, agences gouvernementales etc.) pour lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit etc. Il peut se faire par courriel ou via des sites web falsifiés. C'est donc une forme d'attaque reposant sur l'ingénierie sociale.

Porte dérobée :

Une *porte dérobée*, ou *backdoor* (en anglais) représente une fonctionnalité cachée, inconnue de l'utilisateur légitime et qui donne l'accès à son insu à sa machine. Il s'agit la plupart du temps d'un code malicieux (un petit programme) s'exécutant en toile de fonds. Très souvent, cette astuce est mise en œuvre avec des périphériques malicieux, mais peut aussi être exécuté à distance (typiquement un faux lien URL dans un courriel piégé [phising]) Ainsi, le pirate peut se tenir à jour et porter une nouvelle attaque.

Service d'agrégation :

Un *service d'agrégation de l'information* ou *agrégateur* est un outil et une fonctionnalité généralement intégré dans les réseaux sociaux, blogs, sites Web, etc., qui permet à l'utilisateur d'obtenir les dernières informations concernant un centre d'intérêt particulier. L'agrégateur va alors regrouper et recouper des informations connexes provenant de plusieurs sources (comme par exemple avec les tweets de *Twitter*) pour ne présenter à l'usager que le résultat final.

Spear-phising :

Le *spear-phishing*, ou *harponnage* (en français) est une technique de *social engineering* qui est une variante du phishing ou *hameçonnage* (cf. définition ci-dessus). Elle se focalise sur un nombre très petit d'individus, généralement un seul avec un courriel au contenu fortement personnalisé.

Système cryptographique :

Dans le contexte de la cryptographie (cf. définition ci-dessus), un système cryptographique est alors constitué de trois algorithmes : un pour la génération des clés, un pour l'encryption du message et un pour le déchiffrement du message. Le but étant d'assurer *la confidentialité*, *l'intégrité* et *l'authenticité* du (des) messages(s) échangé(s).

Système de détection d'intrusion :

Un *système de détection d'intrusions* (ou *IDS* : de l'anglais *Intrusion Detection System*) est un périphérique ou processus actif qui analyse l'activité du système et du réseau pour détecter toute entrée non autorisée et/ ou toute activité malveillante. Il existe également des systèmes de prévention d'intrusion (*IPS*). L'idée est de prévenir une éventuelle attaque avant que les ressources ne soient vraiment endommagées.

Zone démilitarisée :

Dans le contexte de la sécurité informatique, une *zone démilitarisée*, ou demilitarized zone (en anglais) désigne une partie du réseau d'entreprise qui est isolé d'internet par un pare-feu. Cette partie spécifique du réseau contient généralement tous les services susceptibles d'être accédés par l'extérieur (c'est-à-dire internet). Ainsi, en cas d'attaque, cette dernière est contenue dans cette sous-partie du réseau de l'entreprise et évite la propagation à l'ensemble de l'infrastructure interne. Généralement on place uniquement une copie (un miroir) du site d'entreprise dans cette zone. La version « originale » se trouvant hébergée dans le réseau interne de l'entité. Ce qui permet notamment de restaurer plus rapidement le service aux usagers.

Bibliographie

Livres (monographies) :

- BLOCH, Laurent, WOLFHUGEL, Christophe : *Sécurité Informatique : Principes et méthode*. Eyrolles. Paris : 2007, 261 p.

- D. MITNICK, Kevin, L. SIMON, William. *The art of deception : Controlling the Human Element of Security*. Wiley Publishing, Inc. Indianapolis, Indiana : 2002, 352 p.

- GOMEZ-URBINA, Alexandre : *Hacking Interdit 4ème édition*. Micro Application. Paris : 2010, 477 p.

- HADNAGY, Christopher. *Social Engineering : The Art of Human Hacking*. Wiley Publishing, Inc. Indianapolis, Indiana : 2011. 408 p.

- JACQUET, Laurent. *Lexique du renseignement, de l'information et de l'influence*. L'Esprit du Livre Editions. Paris : 2010, p.128

- MANISH, Gupta, RAJ, Sharman : *Social and Human Elements of Information Security*. Information Science Reference, New-York : 2009, 412 p.

- MANN, Ian. *Hacking The Human : Social Engineering Techniques and Security Countermeasures*. Gower. Burlington (USA) : 2008, 254 p.

- MUSSET, Jöelle : *Sécurité Informatique : Ethical Hacking : Apprendre l'attaque pour mieux se défendre*. Editions ENI. France : 2009, 355 p.

Articles de périodique :

- ANUBHAV, Chitrey et al. A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. *International* Journal of Information & Network Security *(IJINS)*, 2012, vol. 1, no 2, pp.45-53

- BARRETT, Neil. Penetration testing and social engineering : Hacking the weakest link. *Information Security Technical Report*, 2003, vol. 8, no 4, pp.56-64

- BEAVER, Kevin. Social Engineering : The big risk no one's thinking about. *Security Technology Executive*, 2009, vol. 19, no 4, p.35

- CRESSON WOOD, Charles. Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security*, 2004, vol. 2004, no 1, pp. 16-17

- FURNELL, Steven, ZEKRI Leith. Replacing passwords : in search of the secret remedy. *Network security*, 2006, vol. 2006, no 1, pp. 4-8

- MEGHA, Gupta, SAMEER Agrawal. A survey on social engineering and the art of deception. *International Journal of Innovations in Engineering and Technology (IJIET)*, 2012, vol. 1, no 1, pp. 31-35

- MUNRO, Ken. Social Engineering. *Infosecurity Today*, 2005, vol. 2, no 3, p.44

- PHILPOTT, Andrew. Identity theft – dodging the own-goals. *Network security*, 2006, vol. 2006, no 1, pp. 11-13

- RAJ, Samani. Re-defining the human factor. *Infosecurity*, 2010, vol. 7, no 2, pp. 30-33

- TOWNSEND, Kevin. The art of Social Engineering. *Infosecurity*, 2010, vol. 7, no 4, pp. 32-35

Articles de conférences :

- Rössling, Guido et Müller, Marius : *Social Engineering : a serious underestimated problem,* Proceedings of the 14th annual ACM SIGCSE conference on innovation and technology in computer science education, ITiCSE '09, ISBN 9781605583815, p.384 (Paris, France — July 06 - 09, 2009)

Articles électroniques :

- CHENXI, Wang. Your Anti-Social Behavior Stops Here – Set Guidelines To Adopt Social Media And Reduce Risk. In : Forrester [en ligne]. http://www.forrester.com/home#/Your+AntiSocial+Behavior+Stops+Here+Set+Guidelines+To+Adopt+Social+Media+And+Reduce+Risk/quickscan/-/E-RES60188 (consulté le18.04.2013)

- CHENXI, Wang. To Facebook Or Not To Facebook – A social Computing Report. In : Forrester [en ligne]. http://www.forrester.com/home#/To+Facebook+Or+Not+To+Facebook/quickscan/-/E-RES56090 (consulté le 18.04.2013)

- DINESH, Shetty. Social Engineering – The Human Factor. In : Packet Storm [en ligne].

  http://dl.packetstormsecurity.net/docs/social-engineering/the_human_factor.pdf (consulté le 10.07.2012)

- J. HADNAGY, Christopher et al. Sociale Engineering Capture the Flag Results – Defcon 18. In : Social Engineering – Security Through education [en ligne]. http://www.social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf (consulté le 15.10.2012)

- J. HADNAGY, Christopher, O'GORMAN, James. Sociale Engineering Capture the Flag Results – Defcon 19. In : Social Engineering – Security Through education [en ligne]. https://www.social-engineer.com/downloads/Social-Engineer_Defcon_19_SECTF_Results_Report.pdf (consulté le 15.10.2012)

- J. HADNAGY, Christopher, MAXWELL, Eric. Social Engineering Capture the Flag Results – Defcon 20. In : Social Engineering – Security Through education [en ligne]. http://www.social-engineer.org/resources/sectf/Social-EngineerDefcon20SECTFResultsReport-Final.pdf (consulté le 15.10.2012)

- *The Risk of Social Engineering on Information Security : A Survey of IT Professionals.* In : Dimensional Research [en ligne]. http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf (consulté le 20.10.2012)

- *The Ultimate Guide to Social Engineering*. In : CSO Security and risk [en ligne]. http://assets.csoonline.com/documents/cache/pdfs/Social-Engineering-Ultimate-Guide.pdf (consulté le 12.03.2013)

- *15th Annual : 2010/2011 – Computer Crime and Security Survey*. In : CSI : Computer Security Institute [en ligne]. https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf

  (consulté le 15.10.2012)

Pages Web :

- Ingénierie sociale (securité de l'information). In : *Wikipédia* [en ligne]. Dernière modification de cette page le 12 juin 2013 à 22 :09. http://en.wikipedia.org/wiki/Social_engineering_(security) (consulté le 07.07.2012)

- Social Engineering (security). In : *Wikipédia* [en ligne]. Dernière modification de cette page le 14 juin 2013 à 08 :03. http://en.wikipedia.org/wiki/Social_engineering_(security) (consulté le 07.07.2012)

Norme :

- INTERNATIONAL ORGANISATION FOR STANDARDIZATION (ISO). *Information technology – Security techniques – Information security management systems – Requirements.* 1er éd. London : ISO, 2005. 44 p. Norme internationale ISO/IEC 27001:2005

Annexe 1
Exemples d'attaques de *social engineering*

MUSSET, Jöelle : *Sécurité Informatique : Ethical Hacking : Apprendre l'attaque pour mieux se défendre*. Editions ENI. France : 2009, pp.68-72

Exemple n°1 :

Bleck79 est un pirate qui manque de reconnaissance. Pour réussir à être reconnu de ses pairs, il décide de réaliser un exploit : il veut réussir à se faire appeler sur son portable pour un souci d'ordinateur, et ce, depuis l'intérieur des bureaux d'une grosse entreprise dont l'un des pôles est la sécurité informatique.

ArpègeInfo .- « ArpègeInfo, bonjour. »

Bleck .- « Bonjour Monsieur, ici Jean ROBERT de l'URSSAF, puis-je entrer en relation avec votre service Ressources Humaines ? »

ArpègeInfo .- « Bien sûr, ne quittez pas, je vous mets en relation. »

Ressources Humaines .- « Bonjour. »

Bleck .- « Bonjour Madame, nous sommes dans les déclarations concernant votre entreprise, et nous aimerions savoir quel est le dernier employé arrivé chez vous, il s'avère que j'ai un doute sur l'arrivée de certaines déclarations, je pense qu'elles ont été perdues. »

Ressources Humaines .- « Voilà qui est gênant. Notre dernier employée arrivée est Claire PASCALE, elle est là depuis quelques jours seulement, peut-être n'avez-vous tout simplement pas encore reçu la déclaration ? »

Bleck .- « Eh bien non, c'est de ma faute, j'ai la déclaration sous les yeux, j'aurai dû lire la date avant de vous appeler, il y a peu de chances que vous ayez embauché d'autres personnes entre-temps ! »

Ressources Humaines .- « Pas de problème, bonne journée à vous. »

cf. la suite de l'exemple ci-dessous.

Exemple n°1 (suite et fin):

Bleck raccroche et recompose le numéro du standard.

ArpègeInfo .- « ArpègeInfo, bonjour. »

Bleck .- « Bonjour Monsieur, j'aurai voulu joindre Claire PASCALE s'il vous plaît. »

ArpègeInfo .- « Bien sûr, ne quittez pas, je vous mets en relation. »

Claire Pascale .- « Oui, allô ? »

Bleck .- « Bonjour Claire, ici Patrick, du service info. On t'a mis au courant des techniques de sécurité, avec l'installation de l'outil ? »

Claire Pascale .- « Pas vraiment, non »

Bleck .- « Ce n'est pas grave, on va l'installer maintenant »

Bleck79 réussit à faire installer par Claire, une employée nouvelle ne connaissant pas encore les procédures et les personnes, un petit logiciel qui dans quelques jours va afficher à l'écran un message d'erreur, et inviter l'utilisateur (Claire en l'occurrence) à demander Patrick en composant un numéro de téléphone. Bleck79 a pris soin d'acheter un téléphone avec une carte SIM utilisable, au moins pendant quelques jours, sans avoir à divulguer son identité.

Exemple n°2 :

Mickael est étudiant en philosophie. Il a toujours fait preuve d'imagination quand il s'agissait de trouver une excuse pour ne pas aller en classe ou pour justifier un écart de comportement, allant même jusqu'à se faire passer pour un surveillant dans une salle de permanence de son lycée.

Quand le père de son amie le lui demande, Mickael est d'accord pour lui trouver des informations sur les plus gros prospects de la S.A. Airelles, société de fabrication et de distribution de vins et spiritueux. Mickael commence par se renseigner sur Internet, durant quelques minutes, et finit par trouver quelques noms : Nicolas DRINCQ, un commercial. Il décide alors d'appeler la société.

Standard .- « Société AIRELLES bonjour, ici Marie, que puis-je faire pour vous ? »

Mickael .- « Bonjour Marie, ici Cédric Goudement, dites-moi j'ai rencontré votre comptable il y a peu, Nicolas DRINCQ, et il y avait aussi un commercial avec nous... »

Standard .- « Pardonnez moi, Nicolas n'est pas notre comptable, en fait c'est lui le commercial, notre comptable se nomme Michel FRANC. »

Mickael .- « Oh, merci de la correction, voilà qui va m'empêcher de faire une bêtise ! Pourrais-je entrer en relation avec Monsieur FRANC ? »

Standard .- « Oui, bien sûr, ne quittez pas. »

Mickael est alors transféré auprès du comptable à qui il va parler en couvrant sa voix.

Comptable .- « Oui, allô ? »

Mickael .- « Salut Michel, c'est Nicolas. Mon variable me semble ridicule ce mois-ci, est-ce que tu saurais me donner quelques informations qui pourraient m'aider, comme des clients sur le départ ou d'autres qu'on n'a pas encore signés ? »

Comptable .- « Oui... tu peux aller chez... »

Michel FRANC indique alors plusieurs noms à Mickael, qui fit un grand plaisir au père de son amie en les lui transmettant.

Annexe 2
Deux exemples de biais supplémentaire

MUSSET, Jöelle : *Sécurité Informatique : Ethical Hacking : Apprendre l'attaque pour mieux se défendre*. Editions ENI. France : 2009, p.63 et p.66

Biais n°1 :

3.2.8 L'intimidation

Dernier levier technique de base, l'intimidation. Le concept est très simple, il s'agit de faire peur à la cible, en créant une situation de doute où la personne va vouloir à tout prix éviter les problèmes.

Sylvie est créatrice de mode indépendante. Tous les jours, elle rencontre des clients potentiels. Dernièrement, l'un d'entre eux lui a fait faux bond en prétextant ne pas avoir pas reçu de sa part l'e-mail de confirmation de commande pour une collection de plusieurs dizaines de créations. Convaincue d'avoir envoyé l'e-mail et que celui-ci a bien été reçu, Sylvie tente de vérifier. Elle se fait assister par Jean, un ami informaticien.

Jevend .- « Société Jevend, bonjour.»

Sylvie .- « Bonjour Madame, je suis créatrice de mode et j'aurais voulu prendre un rendez-vous avec Monsieur MICHEL, pour lui présenter mes créations. »

Jevend .- « Oui, bien sûr. Est-ce que mardi vous convient ? »

Sylvie .- « Ah, mardi tombe plutôt mal. Serait-il disponible lundi ? Je vis un peu au nord de Paris, peut-être est-ce qu'il se déplace dans ce secteur ? »

cf. la suite du biais ci-dessous.

Biais n°1 (suite et fin) :

Jevend .- « Non, monsieur est en déplacement lundi, mais pas dans la région parisienne. Je n'ai malheureusement que mardi à vous proposer, au plus tôt ».

Sylvie .- « D'accord. Bon écoutez, je vais tenter de m'arranger et je vous rappelle pour prendre rendez-vous. Merci beaucoup ! »

Jevend .- « Aucun problème, bonne journée à vous.»

Le lundi suivant, Sylvie appelle, elle sait que le patron est absent...

Jevend .- « Société Jevend, bonjour.»

Sylvie .- « Bonjour Madame, je suis standardiste et nos deux directeurs sont en réunion ici. Malheureusement, le vôtre a perdu le mot de passe de sa boîte e-mail et le mien lui a promis qu'on allait pouvoir faire quelque chose, vous et moi. L'ambiance est un peu tendue dans le bureau et j'ai l'impression qu'on risque gros si on n'arrive pas à s'en sortir. Est-ce que par chance vous connaîtriez son mot de passe ? »

Jevend .- « Non, je n'en ai aucune idée. Peut-être y a-t-il un moyen de le récupérer ou de le changer ? »

Sylvie .- « Oui, bien sûr. Mon collègue du service informatique va vous donner la procédure ».

Jean, l'ami de Sylvie, termine la discussion en donnant quelques indications pour récupérer le mot de passe.

Sylvie découvre dans la boîte mail de monsieur MICHEL que son e-mail de confirmation lui est bien parvenu, et en profite pour le passer en statut « Non Lu », pour faire un clin d'œil discret au directeur de la société, dont elle sait maintenant qu'il l'a évincée pour d'autres raisons.

Attaque en deux temps cette fois-ci, avec une première étape où Sylvie localise un créneau pour être sûre de pouvoir dérouler son histoire. La clé, c'est l'impression que l'avis du directeur dépend directement de la réussite de cet appel : si les deux assistantes ne trouvent pas une solution, leur poste est peut-être en jeu. La pression peut être telle dans ces cas-là que les personnes oublient complètement ce qu'il convient de faire ou ne pas faire.

Biais n°2 :

3.2.6 L'altruisme

Dans le social engineering, une méthode intéressante est de susciter chez la cible l'envie de vous aider, inversant presque les rôles dans le sens où les informations vont émaner de la cible, dans le meilleur des cas avant même que l'assaillant ne les demande.

> Coralie est pédopsychiatre dans une petite clinique de Bretagne. Grande adoratrice des enfants, elle supporte difficilement les personnes qui mettent leur vie en danger. A fortiori, elle n'a donc aucune raison d'apprécier son voisin qui roule avec un véhicule de forte puissance, n'hésitant pas à franchir les limitations de vitesse et circulant dans le quartier résidentiel à des vitesses dépassant de loin le raisonnable. Son pare-brise arbore une vignette d'assurance avec un logo représentant une étoile de mer, mais Sandrine est convaincue qu'il s'agit d'un faux.

Assurances Étoiles .- « Assurances Étoiles, bonjour, que puis-je faire pour vous ? »

Coralie .- « Bonjour, je suis de la maison. Je suis en déplacement sur votre région pour le service commercial, et je voudrais vendre une assurance à un assuré qui vient de s'acheter une très grosse voiture... mais voilà, j'ai fait 200 kilomètres, j'ai préparé mon discours commercial toute la nuit et j'ai oublié son dossier chez moi. »

Assurances Étoiles .- « Effectivement, cela va être moins facile que prévu pour le coup. Est-ce que je peux vous le lire, et vous prenez quelques notes ? »

Coralie .- « Moins facile. Je risque de gros problèmes avec mon responsable s'il apprend ça ! De plus, je ne vais pas avoir l'air très sérieuse devant le client avec mes notes manuscrites. »

Assurances Étoiles .- « Si vous aviez un ordinateur, vous pourriez accéder à ClassClient 3.0, mais là, je ne sais pas comment faire. »

Coralie .- « Attendez, je passe près d'une boutique de téléphonie, ils ont forcément un fax. Vous pourriez m'en envoyer un ? »

Assurances Étoiles .- « Oui, si vous me donnez le numéro d'assuré et le numéro du fax je peux vous l'envoyer. »

cf. la suite du biais ci-dessous.

Biais n°2 (suite et fin) :

Coralie .- « Super ! Vous me sauvez la vie, j'aurais peut-être perdu ma place si vous n'étiez pas là. Le numéro est le 01.23.45.67.89 et le dossier concerne un monsieur G.D. À l'adresse... »

Coralie a eu confirmation de ses soupçons : le dossier de cette personne contient la mention d'une assurance voiture mais qui n'est plus payée depuis près de deux ans. Pour une telle cylindrée, le prix est assez exorbitant et Coralie comprend pourquoi son voisin préfère s'abstenir d'être assuré.

Susciter l'envie d'aider est très simple, en réalité. Il suffit de faire croire à l'interlocuteur qu'on se ressemble, et ensuite de se prétendre dans une situation que personne ne voudrait vivre, et dont tout le monde voudrait nous sortir pour peu que cela ne coûte rien, ou presque. Et dans notre exemple, c'est le cas : la standardiste peut aider Coralie qui se trouve dans une position délicate et qu'entre collègues, il est normal de s'entraider. À noter, le numéro de fax est celui d'une boutique quelconque, qui fera payer quelques euros à Coralie pour recevoir le fax. L'anonymat n'est pas plus coûteux que ça.