Pirater l'humain

L'analyse du phénomène d'ingénierie sociale

David Castonguay

Note de recherche no. 4

Chaire de recherche du Canada en sécurité identité technologie

Université de Montréal

Ce travail a été réalisé dans la cadre du cours CRI-6234, « Nouvelles technologies et crimes » (session d'automne 2009), offert aux étudiants de la Maîtrise en Criminologie sous la direction du Professeur Benoît Dupont.

La Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal mène des études sur les pratiques délinquantes associées au développement des technologies de l'information, ainsi que sur les mécanismes de contrôle et de régulation permettant d'assurer la sécurité des usagers.

David Castonguay
david.castonguay1@gmail.com

Prof. Benoît Dupont
Centre International de Criminologie Comparée (CICC)
Université de Montréal
CP 6128 Succursale Centre-Ville
Montréal QC H3C 3J7 - Canada
benoit.dupont@umontreal.ca
www.benoitdupont.net
Fax : +1-514-343-2269

Table des matières

INTRODUCTION

Le développement des nouvelles technologies de l'information et de la communication ont grandement modifié les pratiques en matière de sécurité. Lorsque l'on parle de protection de l'information, les solutions technologiques se sont avérées un choix logique et efficace. Par contre, cette tendance à appliquer une solution technologique a eu pour effet pervers de négliger le facteur humain. Peu importe à quel point un système de sécurité est sophistiqué et complexe, il y aura toujours un être humain pour contrôler ce système. Dans son environnement de travail, de tous les jours, l'humain doit faire des choix et prendre des décisions qui peuvent avoir des conséquences importantes pour la sécurité de l'entreprise. Si l'humain est l'élément central de toute organisation, il représente également l'élément le plus vulnérable, car il est à la fois la cause de nombreux incidents et la partie maîtresse dans la protection de l'information. Faisant partie à la fois de la solution et du problème, il est essentiel de s'attarder à son comportement et de comprendre pourquoi il est vulnérable. En fait, il est surprenant de constater à quel point l'élément humain est vulnérable et facilement exploitable. L'ingénierie sociale, qui est l'art d'utiliser la tromperie et le mensonge pour arriver à ses fins (Mitnick, 2006), exploite précisément ce maillon faible de la chaîne de sécurité.

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

L'ingénierie sociale est une attaque peu coûteuse, qui ne nécessite pas de recours à la force ou de violence, relativement accessible à tous, bien qu'elle demande certaines aptitudes sociales et furtives. Afin de faire face à cette menace, il est nécessaire de mieux comprendre le processus décisionnel en matière de sécurité ainsi que des éléments qui influencent ce processus. Selon moi, la première étape pour faire face à l'ingénierie sociale est une prise de conscience des mécanismes sous-jacents à cette menace. Une meilleure compréhension et une modélisation des différentes composantes de l'ingénierie sociale permettront la mise en place de solutions adaptées. Ce travail se concentre sur l'ingénierie sociale utilisée dans le cas de communication téléphonique ou en personne.

Il est divisé en deux sections. Tout d'abord, je vais identifier les éléments qui provoquent des erreurs de jugement lors de la prise de décision en matière de sécurité. Ensuite, j'aborderai les facteurs sociologiques à la base de l'ingénierie sociale.

RECENSION DES ÉCRITS

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

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

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

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

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

Bien qu'il soit difficile d'évaluer la prévalence de l'ingénierie sociale comme menace à la sécurité, plusieurs exemples populaires illustrent bien la crédibilité de la menace. À ce titre, Kevin Mitnick est l'un des pirates informatiques les plus célèbres, car celui-ci a été le premier à figurer sur la liste des dix personnes les plus recherchées par le FBI à la fin des années 1980. Il a piraté les bases de données de clients de Pacific Bell, de Fujitsu, Motorola, Nokia, Sun Microsystems, en plus d'accéder illégalement à un ordinateur du Pentagone. Mitnick, maintenant conseiller en sécurité de l'information, utilisait principalement l'ingénierie sociale, notamment par téléphone ou en personne, afin d'obtenir l'accès nécessaire au système. Ainsi, il a démontré qu'il est beaucoup plus simple de manipuler les gens afin d'obtenir l'information désirée plutôt que pirater les barrières de sécurité informatique. Ses livres, *The Art of Deception: Controlling the Human Element of Security* (2003) et *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (2005), illustrent bien l'efficacité de l'ingénierie sociale ainsi que le potentiel qu'elle représente. Cependant, il importe ici de faire la différence entre les attaques qui sont possibles (réalisées) et celles qui sont probables (imaginées). Cette distinction permettra de s'éloigner des récits qui tiennent davantage de l'anecdotique que de la réalité.

Mais l'humain n'est pas simplement vulnérable à la manipulation. Car les études empiriques en psychologie cognitive ont démontré que même si l'humain possède toutes les informations nécessaires pour prendre une décision éclairée et qu'il est totalement en contrôle de son environnement, il prendra, dans la majorité des cas, tout de même la mauvaise décision. En introduisant la psychologie cognitive à cette recherche, je souhaite aller à la source de ces erreurs de raisonnement afin d'identifier les éléments vulnérables pour le domaine de la sécurité.

Les recherches sur la psychologie cognitive étudient comment les individus perçoivent, apprennent, se souviennent et pensent l'information qu'ils reçoivent (Launay, 2004). Il s'agit de l'étude des processus mentaux impliquée dans l'acquisition et l'utilisation des connaissances humaines (Launay, 2004 : 13). Chaque jour, l'humain fait face à des choix qui impliquent une évaluation ainsi qu'une prise de décision. Différents facteurs jouent un rôle dans la prise de décision et dans le processus de raisonnement.

De prime abord, l'humain est une espèce très intuitive. Lorsqu'il traite de l'information, il arrive fréquemment que le cerveau saute à la conclusion et qu'il prenne des décisions presque instantanément. L'inconscient est une force prodigieuse, mais il n'est pas infaillible. Dans son ouvrage Blink, Malcolm Gladwell (2006) démontre comment, dans le quotidien l'humain, fait des conclusions hâtives et comment l'inconscient de son cerveau fonctionne dans des situations précises. Fortement inspiré par la théorie de l'évolution, cet écrivain s'inspire de nombreuses recherches universitaires en sociologie et psychologie afin de démontrer comment l'expérience passée influence notre perception de la situation et notre prise de décision.

De plus, dans les situations complexes, il est très rare que l'on possède toutes les informations nécessaires afin de prendre une décision optimale. La capacité de raisonnement est donc limitée aux solutions connues. En fait, même si l'humain possédait toutes les informations possibles et disponibles, il ne pourrait pas traiter toute l'information, car il a une rationalité limitée, c'est-à-dire qui opère dans certaines limites. Cette notion développée par Hebert Simon (1957) démontre que lors d'une prise de décision, pour diverses raisons, une personne ne peut pas considérer toutes les options et que par conséquent, elle choisira l'option la plus satisfaisante et non la solution la plus optimale. Cette théorie s'applique aussi bien à la psychologie qu'à la sociologie. Elle prendra l'option qui lui permet de maximiser ses gains et de réduire ses pertes. Dans cette évaluation, plusieurs critères subjectifs viennent également réduire l'efficacité du raisonnement.

Tversky et Kahneman (1974) se sont intéressés au processus décisionnel qui amène un individu à prendre des décisions grandement inférieures à la solution optimale. Tversky et Kahneman (1974) notent que les individus font souvent appel à des raccourcis mentaux, voire même des biais, qui limitent et parfois déforment notre aptitude à prendre des décisions rationnelles (Sternberg, 2007). Ces biais mentaux, appelés heuristiques, sont utilisés fréquemment dans les prises de décision quotidiennes, car elles sont plus simples et rapides. Par contre, elles mènent généralement à un mauvais raisonnement et à des erreurs dans la prise de décision. Les heuristiques entraînent des déviations systématiques et prévisibles d'un choix rationnel qui peuvent être facilement exploitées par quelqu'un qui est conscient de ces faiblesses. Les heuristiques sont à différencier l´erreur qui est aléatoire, alors que les biais présentent un déterminisme qu´il faut cerner. Par exemple, les biais par excès de confiance influencent notre

perception du risque et le biais de la disponibilité influence l'évaluation de la fréquence et de la probabilité d'un événement.

Si les biais de raisonnement sont à la base des erreurs de jugement, c'est généralement par l'activation de normes sociales que les attaques se matérialisent. Les gens ont besoin des heuristiques afin de prendre des décisions efficaces. Cependant, les heuristiques peuvent être utilisées pour influencer et manipuler les gens. Cialdini (1993) décrit dans son livre *Influence,* six grands principes de la manipulation, qui seront abordés plus tard, fréquemment utilisés dans l'ingénierie sociale.

Comme nous le verrons, plusieurs biais dans la prise de décision résultent d'un processus social. Les sociétés modernes sont régies par un ensemble de normes formelles et informelles qui gouvernent et dictent les comportements à suivre. Ces normes informelles, qui sont des acquis sociaux, ne doivent pas être sous-estimées, car elles causent très souvent des automatismes. En fait, ces principes structurent d'une manière indirecte la prise de décision, car ils créent des automatismes qui sont identifiables et exploitables. Plusieurs de ces normes sociales sont nécessaires au bon fonctionnement de nos sociétés, mais elles représentent également des vulnérabilités. Bref, si certaines sources d'erreur de jugement peuvent être considérées comme individuelles, une proportion non négligeable est socialement induite.

Ce travail vise à répondre aux trois questions suivantes : Comment l'ingénierie sociale exploite-t-elle le processus décisionnel de l'humain afin d'obtenir l'information souhaitée? Quels sont les éléments psychologiques utilisés par l'ingénierie sociale susceptible de provoquer des erreurs de jugement? Quels sont les principes sociaux susceptibles d'être exploités par l'ingénierie sociale?

MÉTHODOLOGIE

Ce travail est exclusivement de nature théorique et vise à analyser la documentation disponible sur l'ingénierie sociale. Afin d'appuyer mes propos, je présenterai plusieurs exemples concrets. Cette méthodologie est la plus accessible et la plus pertinente afin de bien comprendre les mécanismes à l'œuvre dans l'ingénierie sociale. Car bien qu'il s'agisse d'un phénomène répandu, il fait l'objet de peu d'études empiriques. Pour l'instant, la compréhension de l'ingénierie sociale en termes de menace pour la sécurité d'une entreprise n'a pas fait l'objet de beaucoup d'attention scientifique. Par cette étude, je vise davantage à apporter des nouveaux éléments à la compréhension de l'ingénierie sociale qu'à évaluer sa prévalence. La présente étude propose l'analyse de l'ingénierie sociale à travers des dimensions individuelles et sociales dans le contexte particulier de la sécurité.

L'objectif de ce travail est de fournir, aux acteurs de la sécurité, une meilleure compréhension des facteurs sociopsychologiques à la base du fonctionnement de l'ingénierie sociale. Ces derniers seront ainsi conscients des vulnérabilités de l'humain dans sa prise de décision et pourront mettre en place des solutions adaptées à leur environnement.

Prise de décision en sécurité

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

La nature abstraite et subjective de la sécurité complexifie la prise de décision. Ceux qui utilisent l'ingénierie sociale ont bien compris qu'une décision en sécurité résulte d'un calcul coûts bénéfices difficilement opérable mentalement (West, Ryan, Mayhorn, Hardee et Mendel, 2009). Car si on voit généralement peu de bénéfices à prendre une décision sécuritaire, il faut admettre que les coûts sont tout aussi difficiles à évaluer. Tout d'abord, les coûts sont souvent absents, car la menace est invisible. Une personne aimable qui tente de vous aider avec un problème informatique ne représente pas un risque.

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

FACTEURS COGNITIFS

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

Biais de raisonnement

Bien que la prise de décision comporte généralement son lot d'incertitude, notamment face aux risques potentiels d'une décision, la psychologie cognitive a démontré que même si on possède toute l'information nécessaire, on prend souvent des décisions erronées. L'utilisation de

raccourcis mentaux, les heuristiques, lors du traitement de l'information est à l'origine de ses erreurs de jugement. Les heuristiques sont souvent utilisées, car elles sont hautement économiques en temps et en énergie. Par contre, elles mènent à des biais sévères et systématiques. Les heuristiques sont fortement basées sur l'impression qui survient automatiquement et indépendamment de toute évaluation objective de la situation.

Perception du risque et biais d'estimation

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

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

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

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

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

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

La perception du risque est le résultat d'une évaluation subjective. Les études présentées précédemment démontrent que l'humain est influencé et que généralement son évaluation du risque est erronée. Pour une organisation, la perception du risque des employés a un impact majeur sur le comportement qu'ils adopteront face à une situation. Lorsque le risque est sous-estimé, cela entraîne des comportements inadaptés, car les gens n'ont aucun intérêt à se protéger contre cet événement. Il est intéressant de réaliser que, tout le monde, même les responsables de la sécurité sont victimes de ces biais. Il est donc primordial d'en prendre conscience.

Notre raisonnement quant à l'estimation, la probabilité qu'un événement survienne est particulièrement biaisée. L'heuristique de la disponibilité (Tversky et Kahneman, 1974) consiste à fonder nos estimations sur la facilité de récupération en mémoire d'exemples qu'on considère comme pertinents. En fait, on ne cherche pas d'autres informations que celles immédiatement disponibles. L'utilisation de cette heuristique peut amener l'individu à surestimer le poids des dimensions les plus rares de l'événement en raison de leur forte disponibilité en mémoire. Ce biais influence notre évaluation de la fréquence et de la probabilité qu'un événement survienne. Bien évidemment, les occurrences récentes sont plus disponibles que les faits plus anciens. Le pirate qui veut exploiter ce biais va utiliser les événements récents de l'actualité ou un événement marquant afin d'influencer la perception du risque. Pour les gestionnaires de la sécurité, il est intéressant de prendre conscience de ce biais surtout lorsque vient le temps d'évaluer la probabilité d'une menace. Afin de limiter l'impact de ce biais, il est primordial de calculer objectivement, c'est-à-dire avec des faits, la probabilité d'une menace.
On considère, à tort, certains éléments comme représentatifs d'une population. Cette heuristique consiste à estimer la probabilité d'un événement incertain en fonction du degré de similarité avec la population d'où il est extrait et de ses traits plus ou moins saillants. Les avocats sont des personnes strictes, sérieuses et honnêtes. En fait, la cible construit son jugement en se fondant sur la ressemblance de la personne perçue à une personne connue. Ce lien de similarité est fortement nourri par les stéréotypes. Le pirate va utiliser les stéréotypes à son avantage pour avancer ses arguments et influencer le jugement de la cible. Cette heuristique peut également reposer sur l'évaluation d'une fausse relation de cause à effet entre deux événements.

Information confirmatoire

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

BASES DE L'INFLUENCE

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

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

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

Réciprocité

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

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

Engagement et cohérence

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

La cohérence dans les actions et les paroles est considérée comme une preuve d'intelligence. Celui qui change constamment de point de vue n'est pas cohérent avec lui-même. Cela signifie que l'individu continuera à agir en fonction de son engagement initial même si le contexte change. Par exemple, si un inconnu demande à quelqu'un de surveiller son sac alors qu'il va à la toilette et qu'un voleur tente de s'emparer de ce sac, la personne chargée de la surveillance interviendra avec plus de conviction auprès du voleur qui si elle ne s'était pas engagée formellement à surveiller le sac de la personne. Tout cela pour respecter son engagement initial. Il y a une persistance dans le temps de l'engagement car il est généralement mal vu de changer d'idée. Il est difficile de convaincre un individu avec des menaces ou la violence. Pour le pirate, il est beaucoup plus efficace de convaincre la cible et de l'amener à s'engager à effectuer une tâche.

Preuve sociale

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

Autorité

Très jeune, on apprend à répondre positivement à l'autorité, car on réalise qu'il y a des bénéfices à la respecter. L'étude de Stanley Milgram (1974), *Obedience to Authority,* concernant la soumission, est l'une des figures de l'efficacité de l'autorité les plus célèbres. Plusieurs

facteurs viennent influencer ce que l'on perçoit comme une autorité. Il peut s'agir d'uniformes (police, docteur, armée, électricien, maintenance, complet très luxueux), de titres professionnels, d'accessoires (voiture de luxe, cellulaire) ou l'utilisation d'un jargon très précis à un domaine (Cialdini, 1993). L'utilisation de ces symboles d'autorité influence fortement la prise de décision même qu'elle enclenche plus souvent qu'autrement des automatismes. Afin de projeter une image d'autorité, le pirate utilise régulièrement ces instruments de manipulation.

Rareté

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

Lien et similarité

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

CONCLUSION

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

L'objectif premier de la sensibilisation est de conscientiser le personnel face à ce phénomène en leur démontrant, par des exemples concrets, comment il est simple d'abuser de la bonne volonté d'un individu et de ses impacts potentiels sur l'organisation. La sensibilisation, bien qu'imparfaite est une première étape essentielle contre l'ingénierie sociale. Être conscient du phénomène et en comprendre les mécanismes sont un excellent début. Savoir que l'ingénierie sociale provoque des réactions instinctives ou que l'on se sent obliger de prendre une décision, contre son gré, qui donne un avantage à une personne peut permettre à un employé d'identifier une éventuelle situation problématique. Il saura alors qu'il doit prendre du recul sur la situation et prendre le temps de réfléchir à la demande.

Il est impossible de se protéger à 100% contre ce phénomène. Par contre, en utilisation différentes méthodes pour instruire le personnel (multimédia, vidéo, tests, mises en situation, organiser de courte séance de rafraîchissement, installer des affiches, distribuer des dépliants, courriel), il est possible d'élever l'attention du personnel et de le maintenir à un niveau acceptable, ce qui réduit les risques. Les formations peuvent être d'abord dispensées à des groupes spécifiques afin de limiter les coûts. La mise en place de politiques et de procédures contribue également à contrer l'ingénierie sociale, car elles servent de guide objectif. Cependant, elles sont généralement trop nombreuses et complexes pour être efficacement comprises et appliquées. Ayant comme objectif premier de servir de guide aux employés dans certaines situations précises, il importe que les principales politiques et procédures soient clairement définies et efficacement diffuser aux employés. De plus, dans ce contexte, comme dans la majorité des programmes de sécurité, il est essentiel d'avoir l'appui de la haute direction si l'on désire avoir l'impact espéré sur les pratiques des employés. Bref, l'ingénierie sociale profite des comportements exploitables de l'humain pour contourner les systèmes de sécurité. Donc, l'humain est à la fois le problème et la solution. Mais il ne faut surtout pas obliger que tout système de protection repose sur le facteur humain.

ANNEXE 1 – Étude de cas

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

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

Par la suite, il lui fait une faveur (réciprocité), en lui disant qu'il peut régler le problème pour que la cible ne perde pas trop de temps. Mais l'attaquant a un délai de temps très restreint, car il doit partir en vacances (rareté) à la fin de la journée. Avant de partir, il aimerait bien avoir terminé, cette section du réseau de l'entreprise. Cependant, s'il respecte la procédure établie entre les deux compagnies, il ne pourra jamais terminer avant de partir et son patron sera mécontent.

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

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

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

L'une des attaques les plus fréquentes est de simplement attendre à l'extérieur de l'édifice ciblé, lors de la pause, et d'entrer en même temps que tous les autres employés.

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

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

Références

Armor, D. A., et Taylor, S. E. (2002). When predictions fail: The dilemma ofunrealistic optimism. In D. Gilovich, D. W. Griffin, & D. Kahneman (Eds.), *Heuristics and biases: The psychology of intuitive judgment*, pp. 334-347.

Cialdini, B. Robert (1993) *Influence: The psychology of persuasion,* Revised edition, 320 p.

Dalziel, J. R., & Job, R. F. S. (1997). Motor vehicle accidents, fatigue and optimism bias in taxi drivers. *Accident Analysis & Prevention, 29*, 489-494.

Dejoy, D.M. (1987). The optimism bias and traffic safety. In *Proceedings of the Human Factors and Ergonomics Society* (Vol. 31, pp. 756-759).

Dontamsetti, Mahi et Anup Narayanan (2009) Impact of the human element on information security, dans *Social and Human elements of information security: Emerging Trends and countermeasures,* édité par Manish Gupta et Raj Sharman, 15-26.

Guéguen, Nicolas (2004). Psychologie de la manipulation et de la soumission, DUNOD, 303 p.

Hammond, K. R. (2000). *Judgments under stress*. New York: Oxford University Press.

Kray, J., et Galinsky, A. D (2003). The debiasing effect of counterfactual mind-sets: Increasing the search for disconfirmatory information in group decisions. *Organizational Behavior and Human Decision Processes*, *91*, 69-81.

Launay, Michel (2004), *Psychologie cognitive,* Hachette Supérieur, 238 p.

Launay, Michel (2004) *Psychologie cognitive,* (eds) Chapitre 5. Processus cognitifs : langage, raisonnement et décision, Hachette Supérieur, 44-176.

Levine, R. (2003). *The power of persuasion*. Hoboken, NJ: John Wiley & Sons Inc.

Long, Johnny (2008) *No tech hacking*, Syngress, 101-117.

Marett, K., Biros, D., & Knode, M. (2004). Selfefficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training. *Lecture Notes in Computer Science, 3073*, 187-200.

Mitnick, Kevin (2003) *The Art of Deception*, *Controlling the Human Element of Security*, 352 p.

Mitnick, Kevin (2005) *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*, 270 p.

Nohlberg, Marcus (2009) Why human are the weakest link?, dans *Social and Human elements of information security: Emerging Trend sand countermeasures,* édité par Manish Gupta et Raj Sharman, 15-26.

OFFICE OF FAIR TRADING (2009) *The psychology of scams : Provoking and committing errors of judgement*, 260 p.

Reason, J. (2002). *Human error.* Cambridge, UK: Cambridge University Press.

Simon, H. (1956). Rational choice and the structure of the environment. *Psychological Review*, *63*, 129-138.

Sternberg, Robert (2007). *Manuel de psychologie cognitive : du laboratoire à la vie quotidienne,* De boeck université, 664 p.

Taylor, S. E., et J. D. Brown (1988). Illusion and well-being: A social psychological perspective on mental health. *Psychological Bulletin*, *103*, 193- 210.

Tversky, A, et D. Kahneman, (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124-1131.

West, Ryan; Mayhorn Christopher; Hardee Jefferson et Jeremy Mendel (2009) The weakest link: A Psychological perspective on why users make poor security decisions, dans *Social and Human elements of information security: Emerging Trends and countermeasures,* édité par Manish Gupta et Raj Sharman, 43-60.