Social engineering & triangle de la fraude

LES DÉFIS DE LA SÉCURITÉ AU CENTRE DE LA DIMENSION HUMAINE

OLIVIER CARDINI

CEO C.CONSULTING ASSISTANCE
Depuis 1996
Intelligence économique
Anticipation/ développement
Protection
En plaçant l'humain au coeur de la réflexion

PHIL JNH

Consultant spécialisé sûreté et stratégie au profit des entreprises et des particuliers
France et international
32 ans Ministère de la Défense
10 ans secteur privé
CEO BYS BE YOURS SHIELD

CONTACT

Phil JNH sur Linkedin

CONTACT:

www.cardiniconseils-ie.com/blog

Mars 2024

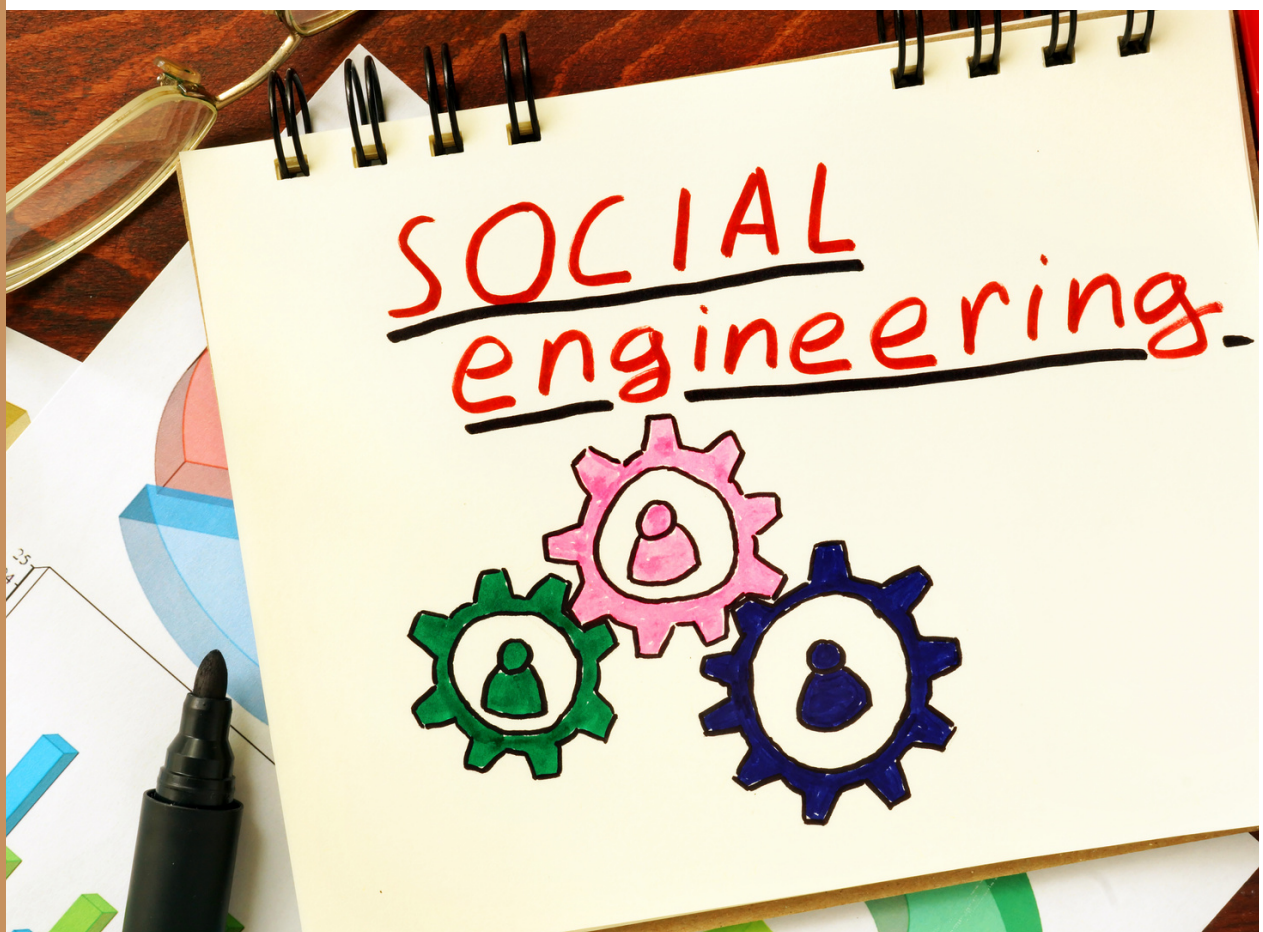
LES DÉFIS DE LA SÉCURITÉ AU CENTRE DE LA DIMENSION HUMAINE

Dans ce domaine complexe de la sécurité, deux sujets émergent avec une force importante, dévoilant des menaces plus vastes et insidieuses : l'ingénierie sociale, où la manipulation devient une arme redoutable, et le "triangle de la fraude", une théorie forgée par Donald Ray Cressey (1919-1987).
Au-delà de ces enjeux, l'ombre grandissante de la cybercriminalité mais également de l'espionnage, impose une exploration approfondie pour comprendre et contrer ces menaces grandissantes.
Depuis ses origines, l'humanité est marquée par un conditionnement binaire, illustré par l'équilibre Yin-Yang ou Bien-Mal, où l'être humain, maillon fort dans divers domaines, se révèle paradoxalement être le maillon faible en matière de sécurité. (1)

POLYBE (203-120 AVV.JC)

« De même qu'un navire privé de son timonier ne tarde pas à tomber dans les mains de l'ennemi avec tout son équipage, de même une armée en opération, si vous dupez son général ou si vous déjouez ses manœuvres, tombera tout entière entre vos mains. »

L'être humain épanoui cherche à atteindre son bien-être personnel, familial, professionnel et social, mais peut involontairement ou consciemment causer du tort ou blesser autrui, car "l'enfer est pavé de bonnes intentions" (proverbe). Les qualités humaines et les valeurs qui guident nos actions déterminent leurs conséquences, et notre capacité de réflexion peut parfois engendrer des intérêts personnels néfastes pour les autres. (2) (3)



L'INGÉNIERIE SOCIALE ... CE POUVOIR D'INFLUENCE INÉGALÉ

L'ingénierie sociale, souvent qualifiée de "piratage psychologique", transcende les attaques informatiques classiques. Ici, point de gadgets sophistiqués, mais plutôt une connaissance approfondie des faiblesses humaines. C'est un jeu où les esprits humains sont les pions, et la compréhension des émotions, le maître-atout.
Imaginez l'ingénierie sociale comme une recette complexe, concoctée avec des ingrédients provenant de la psychologie, mais aussi des sciences sociales et beaucoup du terrain.
C'est une technique subtile, qui requiert non seulement des connaissances, mais aussi et surtout, une expérience fine de « l'humain » dans son application concrète, hors des cadres, loin des salons.
Face aux cyberattaques, il est crucial de maintenir des efforts soutenus et continus en matière de formation et de sensibilisation pour limiter les comportements néfastes, car des individus malveillants seront toujours prêts à causer des dommages importants pour des raisons de vengeance ou d'argent. Le proverbe "Mieux vaut prévenir que guérir" illustre parfaitement cette nécessité. (4)

Entre ubiquité et polyvalence, l'ingénierie sociale n'est pas confinée aux recoins du cyberespace. Elle s'insinue dans tous les aspects de notre quotidien, façonnant la politique, le commerce, le marketing, et nos interactions sociales les plus ordinaires. Un outil polyvalent, utilisé consciemment ou non, de manière intuitive ou élaborée, de manière à visée négative ou positive.
Les conflits et les désaccords mettent souvent en lumière l'influence des intérêts personnels et de l'ego, comme le mentionnait déjà Machiavel dans "Le Prince" en 1513.

« La réalité est le produit du langage que nous employons pour la décrire. »
Wittgenstein

Détecter une attaque d'ingénierie sociale n'est pas comparable à repérer une attaque informatique. Les hackers exploitent la confiance, les émotions, les peurs et les failles organisationnelles. C'est un jeu de patience, de préparation minutieuse et de reconnaissance approfondie.
Oubliez l'image de l'hacker solitaire devant son écran. Les attaquants utilisant ce type de pratique, sont des caméléons sociaux, maîtres dans toutes les situations et dans tous les lieux de votre vie. Leur mémoire visuelle étonnante, leur curiosité, leur créativité, et leur capacité à jouer avec les émotions, simplement avec un téléphone, un mot, un acte non verbal, les classent ... si ce n'était pas pour faire du mal, parmi des acteurs de talent.

« Tromper vraiment consiste d'abord à tromper, puis, ensuite à cesser de tromper. L'illusion croît et atteint son sommet pour laisser place à une attaque en force. Un coup faux, un coup faux, un coup vrai. »
Le n° 7 des 36 stratagèmes (XVe/XVIe siècles)

Se protéger contre l'ingénierie sociale, c'est renforcer les remparts d'un château, pas uniquement l'aspect numérique, mais également dans votre quotidien !
La connaissance est la première ligne de défense. Le défi réside dans notre propre confiance excessive, un point faible que les attaquants exploitent habilement. (5)

UN ACCOMPAGNEMENT PRATIQUE ET CONCRET ... UN IMPÉRATIF EN 2024

« *La vie, ce n'est pas attendre que l'orage passe, c'est apprendre à danser sous la pluie.* » Sénèque

L'efficacité de la formation transcende la théorie, car elle requiert une approche pratique ... davantage que simplement théorique ... Des accompagnants ayant fait l'expérience concrète des différents risques seront essentiels pour guider des apprenants, vers une compréhension et une préparation effective face à ces défis. En matière de sécurité personnelle et physique, il est crucial de se rappeler que la peur de l'arme blanche est souvent infondée. En effet, ce sera davantage l'intention de son porteur, de nuire ou pas, qui fera toujours la différence. À l'époque de nos chers grands-pères, le fameux couteau pliant (l'Opinel ou le couteau suisse) était utilisé pour des tâches simples du quotidien. , Ce qui ne l'empêchait pas d'être également le symbole ou la marque, d'une détermination, d'un certain respect, ou encore d'une simple menace défensive, ce qui est bien loin des actes récurants de notre monde d'aujourd'hui et de sa violence gratuite.

ACCOMPAGNEMENT
SENSIBILISATION
EXERCICES

C'est l'humain, et non l'outil qui penche la balance **vers le négatif ou le positif.** Cette réflexion doit ainsi s'étendre, aussi bien à l'informatique qu'à l'intelligence artificielle. La théorie du "triangle de la fraude" de Donald Ray Cressey (1919-1987) offre un éclairage pertinent dans notre ère de cybermenaces galopantes, mais pas seulement en matière de cybermenaces ...
« **Pression, occasion et rationalisation** » ... Ce triangle expose ces trois éléments interdépendants qui peuvent mener à des pratiques frauduleuses.
La pression initiale, l'occasion créée par des failles, et la rationalisation morale forment un trio explosif ... pas uniquement dans le monde numérique.
Nous avons tous deux facettes : l'être conscient et l'être inconscient, qui influence nos actions et comportements. Le principal danger dans nos prises de décisions réside dans notre propre cerveau et ses failles inconscientes.
Comprendre ces failles est essentiel, bien que surveiller en permanence les erreurs causées par le système 1 soit complexe.
L'introspection et la compréhension de notre processus de réflexion sont des solutions. Par exemple, dans le monde de l'entreprise, le piège de l'ancrage peut être coûteux. Un dirigeant peut être influencé par des prévisions de ventes initiales trop optimistes, conduisant à une surproduction et des stocks excédentaires. Pour déjouer ce piège, l'exercice de "réancrage" consiste à modifier l'ancre initiale en posant des questions ouvertes et en reformulant les informations, activant ainsi le système 2 et limitant les conséquences du piège de l'ancrage.

Comme le montre le principe des systèmes 1 et 2 dans notre processus de décision, (comme le mentionne Daniel Kahneman dans son livre "Thinking, Fast and Slow"), la mauvaise utilisation de la pensée humaine est fréquemment à l'origine de divers problèmes. Dans certaines situations, l'instinct, qui ne prend pas en compte la notion de bien et de mal, peut se montrer plus fiable que la réflexion, comme l'explique Gerd Gigerenzer dans "Rationality for Mortals", ou encore, Malcolm Gladwell dans son ouvrage "Blink : The Power of Thinking Without Thinking".
L'influence sur notre inconscient peut avoir des conséquences insidieuses. Si quelqu'un parvient à agir sur notre inconscient à notre insu, il peut nous manipuler et nous faire croire que ses désirs sont les nôtres.
N'a-t-on pas dit, un jour : **"L'inconscient, c'est le disque dur de l'esprit."**
Pour se prémunir contre de telles manipulations, il est essentiel de développer son esprit critique et d'être conscient des biais cognitifs qui peuvent affecter notre jugement. En étant vigilant et en prenant le temps d'analyser les situations, il est possible de réduire l'impact de ces influences inconscientes sur nos décisions.

Pression et tension : La pression financière très forte avec la conjoncture actuelle, souvent issue de sources professionnelles ou personnelles, crée une tension propice à la fraude. La pression pour une rémunération accrue, alimentée par l'urgence de rembourser des dettes, devient tangible.
Occasion et menaces : Une occasion, née de contrôles inexistants et d'une surveillance défaillante, devient une vulnérabilité exposée. Les attaquants exploitent ces failles, compromettant des données sensibles et semant le chaos financier.
Rationalisation morale : La rationalisation, justifications morales que les fraudeurs se donnent, complète ce triangle. Les pensées du fraudeur évoluent de "C'est temporaire" à des justifications comme "Personne ne sera blessé, après tout !". (7)

Au-delà de l'ingénierie sociale ...

L'ombre grandissante de la cybercriminalité impose une exploration approfondie pour comprendre et contrer ces menaces émergentes. Ces domaines interconnectés exigent une vigilance accrue et une adaptation constante aux évolutions technologiques.
Restez vigilants, adaptez-vous aux évolutions technologiques (IA), et prévenez les risques, avant qu'ils ne prennent racine, mais pas n'importe comment !

Dans le domaine de la sécurité et de la prévention, il est primordial de considérer la dimension humaine, car chaque individu est unique et la sophistication de ses intentions détermine ses actions. **La confiance et la croyance ne vont pas toujours de pair, et il est essentiel d'en tenir compte dans l'élaboration des stratégies.**

« *La guerre, c'est l'art de duper. C'est pourquoi celui qui est capable doit faire croire qu'il est incapable. Celui qui est prêt au combat doit faire croire qu'il ne l'est pas.* »
Sun Tzu (l'Art de la guerre)

Références :

- (1) Rousseau, J.-J. (1762). Émile ou De l'éducation.
- (2) Freud, S. (1913). Totem et tabou.
- (3) Hobbes, T. (1651). Léviathan.
- (4) Moore, T. (2010). The Psychology of Computer Criminals.
- (5) Machiavel, N. (1513). Le Prince.
- (6) Jung, C. G. (1931). L'Homme à la découverte de son âme.
- (7) Elias, N. (1939). La Civilisation des mœurs.