Travail de session

Attaquer le maillon faible de la chaine : L'ingénierie sociale à l'ère du numérique

Travail présenté par

Alex Gravel (20095881)

alex.gravel@umontreal.ca

À

Masarah Paquet-Clouston

Dans le cadre du cours

CRI-6228 – Criminalités Économiques

Université de Montréal

Avril 2022

Résumé exécutif

L'ingénierie sociale est un phénomène qui pose un risque important en cybersécurité. Alors que le nombre d'attaques impliquant des *malwares* ou des *ransomwares* est en forte croissance et que les coûts liés aux brèches de sécurité et aux assurances qui y sont liées sont en hausse (WEF, 2022), on constate que plus de 40% des brèches résultent d'une forme quelconque d'ingénierie sociale (IBM, 2022 ; Verizon, 2021). Il semble donc important de connaître les attaques possibles afin de limiter les vulnérabilités d'une entreprise. À cette fin, le présent rapport définit l'ingénierie sociale et explique son fonctionnement, pour ensuite décrire différents types d'ingénierie sociale (*phishing*, *spear-fishing*, BEC, *pretexting*, quiproquo, *baiting*, *waterholing*, *pharming* et *malvertising*). Enfin, quelques recommandations sont faites pour augmenter la sécurité en entreprise.

Table des matières

L’ingénierie sociale et la fraude

Partie 1 : Introduction

Depuis l’avènement d’internet et des ordinateurs personnels, ceux-ci sont devenus des éléments centraux tant de la vie professionnelle que de la vie personnelle dans les pays développés. Cependant, cette omniprésence de la technologie présente aussi certains risques. Effectivement, elle représente aussi une hausse des opportunités pour la fraude, l’arnaque ou la délinquance en général en ouvrant une nouvelle plateforme pour trouver des cibles et de nouvelles façons pour les criminels d’accéder à celles-ci.

En réponse à la hausse du risque – du *cyber*-risque pour être exact – une nouvelle discipline s’est développée. La cybersécurité a évolué en parallèle aux technologies de l’information, et prend donc ses sources dans les années 70-80 (Eling et al., 2021). Naturellement, depuis cette époque, autant les risques que nos manières de s’en protéger se sont fortement complexifiés et ont gagné en importance. Les enjeux de cybersécurité sont d’ailleurs mentionnés par le *World Economic Forum* ([WEF] ; 2022) comme un des plus importants risques de 2022. Par exemple, seulement en 2020, le nombre d’attaques par *malware* et par *ransomware* ont augmenté de 358% et 435% respectivement ; les frais liés aux assurances contre ces attaques ont augmenté de plus de 200% ; et la fraude bancaire en ligne a augmenté de 117% en volume au Royaume-Uni en 2021 (WEF, 2022). En 2017, les dommages générés par la cybercriminalité étaient évalués à plus de 600 milliards de dollars (Lewis, 2017). Il s’agissait ici de l’évaluation la plus conservatrice que j’ai trouvée.

Lorsqu’on s’intéresse aux causes des brèches de sécurité, on constate toutefois l’importance de l’erreur humaine. En effet, d’après Verizon, plus de 40% des brèches de sécurité en 2020 impliquaient de l’ingénierie sociale (Verizon, 2021). Pour 2021, IBM affirme que le phishing a été

le vecteur initial de 41% des brèches de sécurité (IBM Security, 2022). Il apparaît donc important de se familiariser avec l'ingénierie sociale pour maximiser la cybersécurité de son entreprise.

Le présent travail se concentrera donc sur le phénomène de l'ingénierie sociale et de son lien avec la fraude. Après avoir défini l'ingénierie sociale, j'en présenterai différents types en discutant de leurs avantages respectifs et leur efficacité. Le rapport se terminera par des recommandations pour la prévention de l'ingénierie sociale.

Partie 2: L'ingénierie sociale – Définition

> *Social engineering is the usage of social manipulation and psychological tricks to make the targets assist offenders in their attack* (Bullée et Junger, 2020).

Pour commencer, il semble à-propos de définir l'objet d'étude de ce rapport. Le terme « ingénieur social » (ou plutôt son origine anglophone, « *social engineer* ») a été utilisé pour la première fois dès 1842 par l'économiste John Gray (Hatfield, 2018). À l'époque cependant, le terme était utilisé dans un contexte de politique et d'économie. Il est d'ailleurs intéressant de constater que le *Oxford English Dictionary* comporte deux définitions distinctes pour le terme « *social engineering.* » L'utilisation initiale de l'expression correspond davantage à la première de ces définitions: « *The use of centralized planning in an attempt to manage social change and regulate the future development and behaviour of a society* » (« social engineering, n. », s. d.). On remarque que cette façon de définir l'ingénierie sociale est assez littérale. En effet, on y crée un parallèle avec l'ingénierie en général : l'ingénieur prépare un plan afin de construire ou de modifier une structure. Cette définition est encore utilisée à ce jour.

C'est dans les années 50 et 60 que l'ingénierie social acquiert un deuxième sens. À l'époque, l'accroissement rapide des capacités technologiques a vu apparaître le début du *phone-phreaking*,

où des individus utilisaient différentes techniques de manipulation pour obtenir des bénéfices par téléphone (Hatfield, 2018). Le terme *social engineering* est alors transformé pour indiquer la manipulation d'une cible pour atteindre son propre but. C'est donc suite à ces développements que la deuxième définition du *Oxford English Dictionary* fait surface : « *The use of deception in order to induce a person to divulge private information or esp. unwittingly provide unauthorized access to a computer system or network*» (« social engineering, n. », s. d.).

Hatfield (2018) souligne que ces deux définitions gardent toutefois plusieurs traits communs.

- Asymmétrie de connaissances : le perpétrateur a des connaissances plus avancées que la victime dans le domaine.
- Dominance technocratique : il utilise cet avantage de connaissances pour entraîner un changement de comportement chez l'autre.
- Remplacement téléologique : il arrive à remplacer l'objectif de la cible par le sien.

La définition la plus complète semble être celle de Bullée et Junger (2020) : « *social engineering is the usage of social manipulation and psychological tricks to make the targets assist offenders in their attack* » (Bullée et Junger, 2020). Il est important de mentionner que l'ingénierie sociale n'inclut pas l'utilisation de violence physique, l'extortion, le chantage ou la corruption (Bullée et Junger, 2020).

Processus

Les techniques d'ingénierie sociale suivent généralement un processus en quatre étapes. (« What is Social Engineering », s. d.) Celles-ci sont présentées dans la figure 1. La première phase est celle de l'investigation. C'est à cette étape que l'attaquant identifie sa cible et collecte de l'information

sur elle. Cette collecte peut être faite sur les médias sociaux, en personne, ou via des communications officielles par exemple. La méthode d'attaque est aussi déterminée à ce moment.

La prochaine étape est celle de l'hameçonnage : l'ingénieur social va alors entrer en contact avec sa cible afin de créer une relation de confiance. Son but est d'obtenir une porte d'entrée dans le système. C'est ici que l'ingénieur social présente son prétexte et qu'il prend contrôle de l'interaction.

La troisième phase est l'attaque elle-même. L'ingénieur social renforce sa porte d'entrée en maintenant la relation de confiance et en profite pour accomplir son objectif, soit récolter des données ou installer un *malware* par exemple.

Enfin, l'attaquant doit se sortir de la situation. Idéalement, le tout doit être fait sans laisser de trace. Il doit donc trouver un prétexte naturel pour terminer l'interaction et s'assurer de ne pas laisser de piste physique ou numérique. S'il réussit cet objectif, l'ingénierie sociale est considérée comme un succès et peut être répétée avec d'autres cibles.

Figure 1. *Cycle de l'ingénierie sociale (« What is Social Engineering », s. d.)*

Partie 3 : Techniques et exemples

À travers les années, les techniques d'ingénierie sociale se sont transformées et diversifiées. Plutôt que d'en faire un historique complet, ce travail se concentrera sur les techniques plus récentes, soit celles qu'on a vu apparaître ou gagner en importance à l'ère numérique.

Outre la littérature scientifique et les rapports de firmes de cybersécurité, cette section profite également d'une autre source de données : Reddit[1]. Afin de trouver des exemples et potentiellement d'avoir un indice des dernières tendances d'ingénierie sociale, j'ai rejoint le *subreddit* « r/SocialEngineering ». Cette communauté comprend plus de 145 000 membres. Bien qu'il y ait peu d'activité sur le *subreddit* dans les derniers mois, il s'agit quand même d'une bonne archive. La page présente aussi des suggestions de contenu en lien avec l'ingénierie sociale, incluant des livres, des podcasts et des vidéos, entre autres.

Il est aussi important de mentionner que les différents types d'ingénierie sociale ne sont pas mutuellement exclusifs. Il est tout à fait possible de planifier une attaque ou une campagne jumelant plusieurs des techniques qui seront vues ci-après. Plusieurs brèches de sécurité ne sont pas considérées comme de l'ingénierie sociale, mais y sont souvent reliées ; l'utilisation de *ransomwares*[2], par exemple découle souvent d'une tentative réussie de *phishing* (Verizon, 2021). Le présent rapport ne prétend pas non-plus être une revue exhaustive de l'ensemble des techniques d'ingénierie sociale, mais en présente les plus courantes.

[1] Reddit est une plateforme sociale où les utilisateurs se regroupent par communautés d'intérêts similaires (Subreddit). Ils peuvent alors y publier du contenu (il peut s'agir de liens, d'images, de texte ou de vidéos, par exemple) et ce contenu est ensuite jugé par les autres utilisateurs. Les publications jugées positivement obtiennent une place plus visible sur le fil des utilisateurs et sur les pages des communautés.

[2] Un *ransomware*, ou rançongiciel, est un logiciel intrusif qui bloque l'accès au système qu'il infecte jusqu'à ce qu'une rançon soit payée.

Phishing

La plus classique forme d'ingénierie sociale est le *phishing*. D'après Jakobsson et Myers (2006), le *phishing* se définit comme :

« une forme d'ingénierie sociale dans laquelle l'attaquant, qu'on appelle aussi *phisher*, tente d'accéder frauduleusement aux identifiants confidentiels ou sensibles d'un utilisateur légitime en imitant des communications électroniques d'organisations publiques ou dignes de confiance, souvent de façon automatisée. » (Jakobsson et Myers, 2006, p. 1 ; traduction libre)


Dernier Rappel ! Traitement de votre demande inscription en Ligne Reference : ID- 93758980/2022

Ce courrier a été identifié comme étant du courrier indésirable. Nous le supprimerons prochainement. Courrier légitime

SC Service Client CAF <careersymsli++swedusr@yamaha-motor-india.com>
Mer 2022-04-06 16:04
À : Vous

Droit Individuel à la Formation (DIF)

Madame, Monsieur, Bonjour,

Vos droits de DIF acquis ont été validés et seront crédités au plus tard .

Nous vous informons que nous allons procéder à un contrôle de coordonnées. Dans le cas où vos informations ne sont pas confirmées, votre solde DIF risque de se remettre à zéro.

Nous vous invitons donc à vérifier dès maintenant vos coordonnées justifiant vos DIF acquis:

Accéder au formulaire ici

Cordialement

Répondre | Transférer

Figure 2. *Exemple de courriel de phishing*

L'exemple classique du *phishing* moderne est l'envoi de masse de courriels qui semblent provenir d'un gouvernement ou d'une compagnie connue. Un simple regard dans ma boîte de pourriels m'a permis de trouver l'exemple présenté en figure 2. L'idée générale est d'encourager la cible à donner elle-même ses informations personnelles (Bhardwaj et al., 2020).

La forme la plus simple de *phishing* ferait en sorte qu'en cliquant sur le lien, je me retrouverais sur un site cloné où j'entrerais mes identifiants ou mes coordonnées, qui seraient ainsi diffusées au *phisher*. Les services de courriel infonuagiques sont la cible la plus courante pour ce type

d'ingénierie sociale : on cherche à obtenir l'adresse courriel et le mot de passe de l'individu qui clique le lien (Verizon, 2021). Dans certains cas, l'objectif est plutôt de pousser la personne à cliquer ou télécharger une pièce jointe qui comporte en fait un *malware* s'installant automatiquement sur l'appareil. Il peut donc s'agir d'un *Trojan*[3] ou d'une *backdoor*[4] quelconque (Verizon, 2021).

Le principal avantage du *phishing* est qu'il est extrêmement peu coûteux, tant en ressources qu'en temps. Il peut facilement être automatisé puisqu'il s'agit essentiellement d'envoyer des courriels jusqu'à ce que des gens mordent à l'hameçon (Bullée et Junger, 2020). Un autre avantage est que lorsque le *phishing* est complété avec succès, les compagnies dont la sécurité vient d'être compromise ne s'en rendent souvent même pas compte ; les brèches sont découvertes postérieurement par des organisation externes (Verizon, 2021).

Malgré la simplicité apparente de ces techniques, elles continuent de faire des victimes. Un rapport de 2021 publié par la compagnie Verizon montre une augmentation du nombre d'attaques de *phishing* depuis 2017. On y constate aussi que, dans plus de 18 000 simulations dans des compagnies, le taux de clic (c'est-à-dire se faire avoir par la tentative de *phishing* et cliquer sur le lien) médian est à 3% (Verizon, 2021). Il s'agit d'un taux d'efficacité assez bas. Cependant, certaines études suggèrent que ce taux augmente considérablement selon le contenu du message (Bullée et Junger, 2020 ; Verizon, 2021). Par exemple, la promesse d'un iPad gratuit aurait pour effet d'augmenter le nombre d'hameçonnages réussis (Bullée et Junger, 2020).

[3] Un *Trojan*, ou *Trojan Horse*, est un logiciel malicieux qui est présenté comme inoffensif au premier abord.
[4] Une *backdoor* (porte dérobée en français) est une façon d'infiltrer un système en ignorant ses processus de sécurité et d'authentification.

Bien que le vecteur principal de *phishing* soit les courriels, il peut aussi être mené par messagerie texte (*smishing*) ou vocalement (*vishing*), cette dernière option étant moins facile à faire en masse (Webroot, s. d.).

Spear phishing

Les cyber délinquants ont diversifié les types possibles d'attaque par *phishing* dans les dernières années (Bhardwaj et al., 2020; Webroot, s. d.). Le *Spear phishing* est une sous-catégorie de *phishing* qui est véhiculée de la même façon, mais est beaucoup plus ciblée. Le nombre de messages est diminué au profit de la personnalisation du contenu aux cibles (Caputo et al., 2014). Cette catégorie est en forte croissance, ce qui suggère que les attaquants développent une préférence pour ce type de *phishing*.

Example of a typical campaign	Mass phishing attack (single campaign)	Spear phishing attack (single campaign)
Total messages sent	1,000,000	1,000
Block rate	99%	99%
Open rate	3%	7%
Click-through rate	5%	50%
Conversion rate	50%	50%
Victims	8	2
Value per victim	$2,000	$80,000
Total value from campaign	$16,000	$160,000
Total cost for campaign	$2,000	$10,000
Total profit from campaign	$14,000	$150,000

Figure 3. *Comparaison de l'efficacité d'une campagne de phishing régulière et d'une campagne de spear phishing (Caputo et al. 2014).*

Comme on peut le constater dans la figure 3, une campagne de *spear phishing* comporte beaucoup moins de messages envoyés et ceux-ci sont autant bloqués par les filtres en place (comme le filtre de pourriels et de *spam*). Toutefois, une fois arrivés dans la boîte de réception de la cible, ils ont tendance à être ouverts davantage et les cibles cliquent plus sur les liens ou pièces jointes qui y

sont contenus. Chaque victime est aussi plus payante pour l'attaquant. Cette différence d'efficacité compense largement pour les efforts nécessaires à la mise en place d'une telle campagne (Caputo et al., 2014). Ces données datent toutefois de 2014; il est possible que le portrait ait changé dans les dernières années.

Business Email Compromise

Les *Business Email Compromises* (BEC) sont la forme de *phishing* ayant pris le plus d'expansion dans les dernières années, en plus d'être une des plus dommageables (IBM Security, 2022; Verizon, 2021). La figure 4 montre le gain de popularité de ce type d'attaque parmi les brèches de sécurité liées à l'ingénierie sociale recensées par Verizon (2021). En termes de valeur, le FBI uniquement rapportait en 2018 1,2 milliard de dollars en pertes liée à ce type de fraude (Verizon, 2021). Les pertes totales depuis 2016 pourraient s'élever à 26 milliards de dollars (Saud Al-Musib et al., 2021).

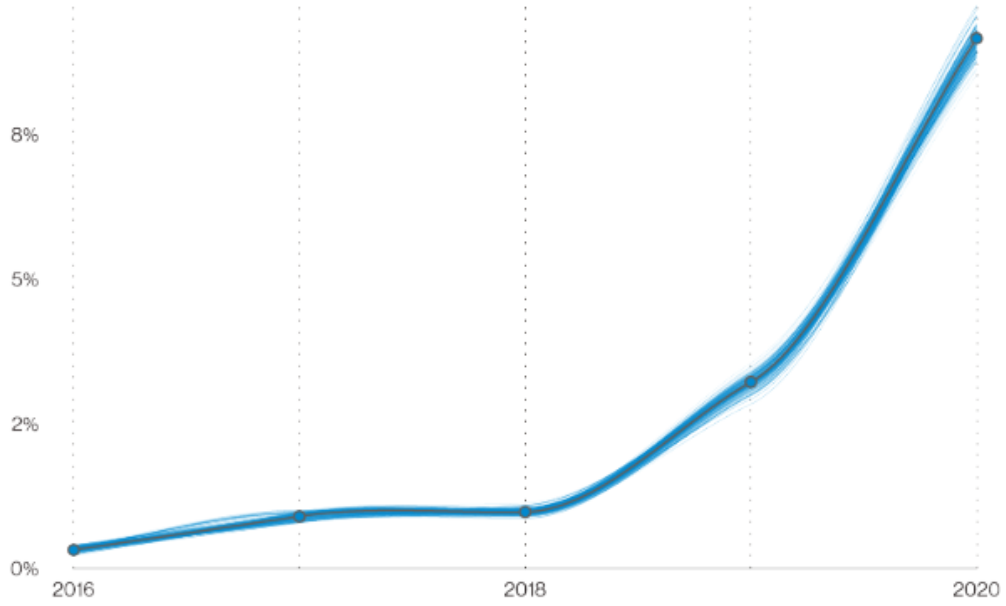

Figure 4. *Fréquence des BEC parmi les brèches de sécurité, excluant les DoS (Verizon, 2021)*

Essentiellement, un BEC implique d'utiliser une adresse courriel semblant appartenir à une figure d'autorité dans une compagnie pour demander ou valider des virements d'argent à des comptes frauduleux appartenant à l'attaquant. Ceci peut être fait de différentes façons. La première possibilité est d'utiliser une adresse similaire à celui de l'autorité (eg. John.smith@hotrnail.com au lieu de john.smith@hotmail.com) pour demander à une personne responsable d'envoyer l'argent au plus vite à un compte spécifique. Alternativement, un résultat similaire peut être obtenu en prétendant être un fournisseur de la compagnie et en envoyant à celle-ci une fausse facture. Enfin, il est aussi possible que les attaquants réussissent à infiltrer les comptes réels des figures d'autorité ou des responsables des transferts monétaires et les utilisent pour procéder aux transferts. Ceci peut résulter d'un *hack* ou d'une fuite de données précédente (Saud Al-Musib et al., 2021).

Les pertes reliées à chaque occurrence de BEC sont considérablement plus élevées que pour le *phishing* classique. Dans le rapport de Verizon (2021), on parle en effet d'un montant médian médian 30 000$USD, avec 95% des incidents comportant des pertes entre 250$USD et 984 855$USD. Verizon (2021) rapporte également que des 19 296 BEC recensés dans l'année 2020, 58% ont été un succès pour l'attaquant.

Pretexting

Le *pretexting* est plus une méthode qu'une attaque en soi. Il est en fait utilisé dans la plupart des attaques d'ingénierie sociale. Il s'agit en fait d'élaborer une histoire (un prétexte) pour justifier la situation en cours (Conteh et Schmick, 2016). Le scénario doit être assez crédible pour mettre la cible en confiance et mettre suffisamment de pression pour qu'elle agisse sans trop réfléchir (Conteh et Schmick, 2016). À cette fin, le pretexting est plus efficace en temps réel, soit en personne ou par téléphone.

Le *pretexting* peut être utilisé seul pour acquérir de l'information ou faire installer quelque chose sur le système de la cible. Le *subreddit* dont il a été question plus tôt, r/SocialEngineering, présente à l'occasion des prétextes utilisés par ses membres. C'est d'ailleurs sur cette page que j'ai été dirigé à l'exemple de cette vidéo : Live hack and social engineering at DEF CON by Dave Kennedy and Kevin Mitnick (le prétexte commence vers 5:00). Il s'agit d'une excellente démonstration, en direct, de comment une interaction de *pretexting* peut se dérouler.

Quiproquo

Le quiproquo ressemble beaucoup au *pretexting*, mais il est plus spécifique. Il s'agit, dans ce cas, de prendre contrôle du système de la cible en prétendant offrir un service. Le quiproquo le plus courant est de prétendre être membre de l'équipe des technologies de l'information de l'entreprise qui est présent pour régler un problème ou pour performer des maintenances par exemple. Son objectif réel est toutefois généralement d'installer un *malware* sur l'appareil en question (Conteh et Schmick, 2016).

Baiting

Le *baiting* a lui aussi l'objectif d'amener l'utilisateur à installer quelque chose sur le système cible. Cette méthode est toutefois différente par son exécution : aucun contact direct n'est pris avec la victime. Le principe de base du *baiting* est de laisser dans un lieu physique un appareil, généralement une clé USB, qui peut contenir un lien ou du code qui s'exécute automatiquement lors de la connexion à un ordinateur. Le système se trouve ainsi infecté par le *malware* et permet à l'ingénieur social d'y accéder (CHUBB, 2014; Krombholz et al., 2015).

Waterholing

Les trois méthodes qui suivent sont un peu plus avancées technologiquement. Pour commencer, le *waterholing* (ou *watering hole attack*) implique de déterminer des pages web qui sont souvent

visitées par la cible et de planter un *malware* sur une de ces pages; éventuellement, la cible devrait être infectée (Krombholz et al., 2015). Cette méthode est plus rare, puisqu'elle nécessite des moyens technologiques plus avancés et bien plus de ressources[5]. Il s'agit donc davantage d'une méthode utilisée par les États à des fins d'espionnage ou les grands groupes de cybercriminels que par des cyberdélinquants et petits groupes. Il est toutefois très difficile de s'en protéger (Allen et al., 2020; Digital Shadows, 2021).

Un exemple assez récent de *waterholing* s'est déroulé en 2019. La campagne *Holy Water,* qui est toujours en cours pour ce qu'on en sait, cible un sous-groupe religieux et ethnique en Asie. Bien qu'on sache que l'opération a eu lieu et que plusieurs appareils ont été infectés, on ignore toujours l'objectif de la campagne et son origine (Kwiatkowski et al., 2021).

Pharming

Le *pharming* (aussi appelé *DNS* poisoning) est aussi une méthode plus avancée d'ingénierie sociale. Il nécessite en fait qu'une faille existe déjà dans le système et n'est donc pas une bonne première étape dans une attaque. L'attaquant profite d'un *malware* déjà présent sur l'ordinateur de la cible ou son *router* pour rediriger son trafic internet vers un site cloné qui semble en tous points similaire au site auquel la victime voulait accéder. Toutefois, toute information fournie sur la page est acheminée aux attaquants (Brody et al., 2007; Webroot, s. d.). À l'instar du *waterholing*, les moyens technologiques nécessaires font en sorte que cette technique et surtout utilisée par les groupes de hackers supportés par l'État (Webroot, s. d.).

[5] Cela est dû au fait que la plupart des attaques de ce type nécessite un *zero-day exploit* pour pouvoir infecter le site en premier lieu. L'information sur une seule de ces vulnérabilités peut se vendre sur le marché noir pour jusqu'à 10 000 000$ USD. Voir le rapport de Digital Shadows (2021).

Malvertising

Finalement, le *malvertising* est similaire aux deux dernières méthodes. La différence est qu'au lieu d'utiliser une faiblesse dans le site web ou dans l'ordinateur de la cible, il attaque seulement une partie des sites webs : les publicités. Le *malvertising* consiste donc à injecter du code malicieux dans des publicités, qui sont ensuite distribués sur des plateformes diverses et réputées comme étant fiables. (Dwyer et Kanguri, 2017; Sood et Enbody, 2011). Les utilisateurs qui cliquent sur ce lien peuvent donc être infectées par un malware sur le coup (Webroot, s. d.), ou même dans certains cas sans cliquer sur le lien (Dwyer et Kanguri, 2017).

Ce type d'ingénierie sociale est plus courant que les deux précédents, mais il est aussi plus facile de s'en protéger. L'utilisation d'un bloqueur de publicités, par exemple, aide à cette protection (Dwyer et Kanguri, 2017).

Plusieurs exemples de *malvertising* peuvent être consultés à cette adresse : https://zeltser.com/malvertising-malicious-ad-campaigns/

Partie 4 : Prévention

Il existe des manières, comme compagnie et comme individu, de se protéger contre l'ingénierie sociale. Dans l'intérêt de ce rapport, je me concentrerai sur les méthodes pouvant être mises en place en entreprise. Elles seront ici présentées sous trois catégories : la formation, les moyens technologiques, et les politiques internes.

Formation

La formation des employés est un point central de la protection contre l'ingénierie sociale. Des programmes comme PhishGuru, NoPhish et PHREE ont montré des bons taux d'efficacité (Bullée et Junger, 2020). Cependant, d'autres études mentionnent que bien que la formation ait des effets

positifs, ceux-ci peuvent être très variables selon des facteurs externes (sociaux, environnementaux, organisationnels, etc.) en plus de ne pas pouvoir s'adapter suffisamment rapidement aux nouvelles campagnes et techniques des attaquants (Aldawood et Skinner, 2019). Elle ne suffit donc pas à une sécurité complète si utilisée seule (Aldawood et Skinner, 2019; CHUBB, 2014).

Le fait d'utiliser des jeux plus dynamiques semble prometteur pour améliorer la qualité de la formation (Boopathi et al., 2015; Scholefield et Shepherd, 2019). Il est aussi recommandé de former les employés dès leur entrée en poste, et de s'assurer qu'ils reçoivent une formation qui correspond à celui-ci (Aldawood et Skinner, 2019). Quelqu'un qui travaille au comptoir d'une entreprise ne verra effectivement pas nécessairement les mêmes types d'ingénierie sociale qu'une personne occupant un poste de bureau. Il est aussi important de s'assurer que la formation soit continue ou répétée régulièrement (Aldawood et Skinner, 2019). Finalement, je recommanderais aussi de sensibiliser les employés aux risques liés aux médias sociaux, qui peuvent être des vecteurs importants d'information pour les ingénieurs sociaux.

Moyens technologiques

Au niveau technologique, plusieurs mesures peuvent aider à la prévention d'attaques liées à l'ingénierie sociale. Beaucoup de moyens existent pour détecter le contenu à risque comme les campagnes de phishing. Les Network-based Intrusion Detection Systems (NIDS) en sont un bon exemple. Certains programmes d'intelligence artificielle existent pour détecter les tentatives d'ingénierie sociale. Ceux-ci démontrent des bonnes capacités de détection, et sont capables de s'adapter aux changements d'adresses et de méthodes des délinquants (Basit et al., 2021).

L'authentification à deux facteurs, bien qu'elle puisse être contournée par certaines techniques, peut aider à renforcer la sécurité des identifiants (« What is Social Engineering », s. d.)

La limitation de certaines fonctionnalités, comme les pièces jointes provenant d'adresses externes ou la géolocalisation des appareils, est aussi considérée comme une bonne pratique. Minimalement, il faut sensibiliser les employés à ne pas utiliser de périphériques trouvés ou venant de sources incertaines (CHUBB, 2014).

Politiques internes

Enfin, certaines politiques internes peuvent augmenter la sécurité de l'information d'une entreprise. D'abord, performer un *Penetration Testing* régulièrement est très important au maintien de la sécurité, en permettant de trouver les faiblesses résiduelles (CHUBB, 2014). Il est aussi recommandé de garder un registre des données sensibles, afin de savoir qui y a accès. Ceci permet de trouver les employés qui représentent des cibles plus intéressantes pour d'éventuels attaquants (CHUBB, 2014). Toute transaction monétaire devrait être sujette à vérification, plutôt qu'être validée par une seule personne, pour éviter les attaques de type BEC (CHUBB, 2014).

Toutes les politiques n'ont pas à être complexes : limiter l'utilisation de périphériques externes comme les clés USB et détruire complètement les documents papiers permet aussi d'éliminer certaines menaces (CHUBB, 2014).

Conclusion

L'ingénierie sociale présente des défis importants, dans un monde où les données sont de plus en plus nombreuses et ont de plus en plus de valeur. La première étape pour se protéger de quelque chose est d'apprendre à la connaître; ce rapport a été produit dans cet objectif. Quelques éléments mériteraient d'être approfondis par des recherches subséquentes, en particulier en ce qui a trait à la prévention. En effet, il serait pertinent de s'informer sur des logiciels spécifiques de protection et leurs avantages, ainsi que sur un modèle plus global de la cybersécurité en entreprise qui inclurait toutes les facettes de prévention abordées ici mais de façon plus intégrée et tenant compte

du contexte d’application. Le présent rapport n’est finalement qu’un bref aperçu des attaques pouvant cibler l’humain derrière l’écran, et n’est donc qu’un point de départ pour approfondir les connaissances sur un domaine vaste et dynamique.

Liste de références

Aldawood, H. et Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073

Allen, J., Yang, Z., Landen, M., Bhat, R., Grover, H., Chang, A., Ji, Y., Perdisci, R. et Lee, W. (2020). Mnemosyne: An Effective and Efficient Postmortem Watering Hole Attack Investigation System. Dans *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (p. 787-802). Association for Computing Machinery. https://doi.org/10.1145/3372297.3423355

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z. et Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139-154. https://doi.org/10.1007/s11235-020-00733-2

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N. et Arthi, S. (2020). Why is phishing still successful? *Computer Fraud & Security*, *2020*(9), 15-19. https://doi.org/10.1016/S1361-3723(20)30098-1

Boopathi, K., Sreejith, S. et Bithin, A. (2015). Learning Cyber Security Through Gamification. *Indian Journal of Science and Technology*, *8*, 8.

Brody, R. G., Mulig, E. et Kimball, V. (2007). Phishing, pharming and identity theft, *11*(3), 14.

Bullée, J.-W. et Junger, M. (2020). Social Engineering. Dans T. J. Holt et A. M. Bossler (dir.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (p. 849-875). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_38

Caputo, D. D., Pfleeger, S. L., Freeman, J. D. et Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security Privacy*, *12*(1), 28-38. https://doi.org/10.1109/MSP.2013.106

CHUBB. (2014). *Guide to preventing social engineering fraud*. https://studium.umontreal.ca/pluginfile.php/7070310/mod_data/content/484052/%5BPlourde%2C%20Maude%20-%20Guide%20to%20preventing%20social%20engineering%20fraud%5D.pdf

Conteh, N. Y. et Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 8.

Digital Shadows. (2021). *Vulnerability Intelligence: Do You Know Where Your Flaws Are?* https://resources.digitalshadows.com/whitepapers-and-reports/vulnerability-intelligence-do-you-know-where-your-flaws-are

Dwyer, C. et Kanguri, A. (2017). Malvertising - A Rising Threat To The Online Ecosystem. *Journal of Information Systems Applied Research*, *10*(3), 29.

Eling, M., McShane, M. et Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125. https://doi.org/10.1111/rmir.12169

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102-113. https://doi.org/10.1016/j.cose.2017.10.008

IBM Security. (2022). *IBM Security X-Force Threat Intelligence Index*. IBM. https://www.ibm.com/security/data-breach/threat-intelligence/www.ibm.com/security/data-breach/threat-intelligence

Jakobsson, M. et Myers, S. (2006). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. John Wiley & Sons.

Krombholz, K., Hobel, H., Huber, M. et Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Kwiatkowski, I., Aime, F. et Delcher, P. (2021, 31 mars). Holy water: ongoing targeted water-holing attack in Asia. *SecureList*. https://securelist.com/holy-water-ongoing-targeted-water-holing-attack-in-asia/96311/

Lewis, J. (2017). *Economic Impact of Cybercrime—No Slowing Down*. Center for Strategic and International Studies.

Saud Al-Musib, N., Mohammad Al-Serhani, F., Humayun, M. et Jhanjhi, N. Z. (2021). Business email compromise (BEC) attacks. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.03.647

Scholefield, S. et Shepherd, L. A. (2019). Gamification Techniques for Raising Cyber Security Awareness. *HCI International*, *2019*, 15.

social engineering, n. (s. d.). Dans *Oxford English Dictionnary Online*. Oxford University Press. https://www.oed.com/view/Entry/272695

Sood, A. K. et Enbody, R. J. (2011). Malvertising – exploiting web advertising. *Computer Fraud & Security*, *2011*(4), 11-16. https://doi.org/10.1016/S1361-3723(11)70041-0

Verizon. (2021). *2021 Data Breach Investigations Report (DBIR)*. https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx

Webroot. (s. d.). *11 Types of Phishing attacks you need to know to stay safe*. https://studium.umontreal.ca/pluginfile.php/7070310/mod_data/content/486064/%5BGuillot%2C%20Robin-11%20Types%20of%20Phishing%20attacks%20you%20need%20to%20know%20to%20stay%20safe%5D%20.pdf

What is Social Engineering. (s. d.). *Imperva*. https://www.imperva.com/learn/application-security/social-engineering-attack/

World Economic Forum. (2022). *Global Risks Report 2022*. https://www.weforum.org/reports/global-risks-report-2022/