Social engineering

L’essentiel en bref

Le « social engineering », une méthode de collecte d'informations dont l'objectif est de manipuler les personnes pour qu'elles autorisent des accès, révèlent des données confidentielles et sensibles, partagent des informations ou déplacent des sommes d'argent. Le « social engineering » ne consiste pas à pirater des systèmes ou à percer des pare-feu (système qui protège un réseau ou un ordinateur contre les accès indésirables via Internet), en effet, c'est l'individu lui-même qui révèle des informations ou effectue une action « de sa propre volonté ». L'ingénierie sociale se produit aussi bien dans le monde analogique, réel, c'est-à-dire lors de rencontres directes avec des personnes, que dans le monde numérique, lorsque l'on communique en ligne (e-mails).

Les méthodes manipulatrices de collecte d'informations existent depuis le début de la civilisation humaine, mais aujourd'hui, le terme social engineering est le plus souvent utilisé dans le contexte de la fraude numérique sur Internet. Nous sommes fortement connectés via Internet et les médias sociaux et de temps en temps, des personnes inconnues nous contactent par ces canaux de communication.

Ingénierie sociale dans le secteur financier

La numérisation rend la plupart des processus plus complexes au sein du secteur financier. Les clients ne sont pas forcément conscients des différentes étapes du processus et peuvent donc facilement être victimes du « social engineering ». Il est particulièrement tentant pour les spécialistes de “social engineering” de tenter leur chance auprès des clients des établissements financiers (banques, assurances), car c'est là que l’argent est éventuellement déplacé.

Comment fonctionne l'ingénierie sociale ?

Les « social engineers » se construisent une fausse identité à partir des informations collectées sur la victime, de sorte qu'ils paraissent suffisamment légitimes. Ils jouent un rôle différent en fonction de ce qu'ils veulent voler à la personne. Cela peut varier d'une connaissance ou d'un employé de banque à un artisan. Sans établir de contact direct, ils utilisent souvent des moyens de communication tels que le téléphone, le courrier électronique ou les SMS. Pour gagner la confiance des gens, les « social engineers » font attention à plusieurs aspects afin d'imiter les comportements humains typiques : ils se font passer pour particulièrement gentils et aimables ou se présentent comme une figure d'autorité dont les instructions doivent être suivies. Ils disent qu'ils ont une demande urgente ou exigent que quelque chose soit fait absolument et rapidement.

Voici quelques exemples :

Phishing (de l'anglais « to phish », en français : pêcher quelque chose) :
Avec les e-mails dits de « phishing », les « social engineers » tentent d'obtenir des mots de passe ou de diffuser des virus / logiciels malveillants (programmes nuisibles). L'e-mail peut, par exemple, contenir

une offre alléchante, une fausse facture ou une demande de mise à jour. L'objectif est d'obtenir une action immédiate, par exemple, que tu révèles des informations, que tu cliques sur un lien ou que tu ouvres une pièce jointe dangereuse.

Le « phishing » peut également se faire par SMS ou par appel téléphonique. Pour les SMS, on parle de « smishing », pour les appels de « vishing ».

Baiting (de l'anglais « to bait », en français : appâter) :
L'attaque par appât : dans ce cas, l'agresseur tente d'attirer la victime avec un appât et espère susciter la curiosité ou même la cupidité de la victime. L'agresseur utilise un appât physique ou numérique qui cache généralement un logiciel malveillant (programme nuisible). Il peut s'agir, par exemple, d'une clé USB avec des contenus apparemment intéressants ou d'un lien de téléchargement qui doit mener à un logiciel sympa.

Pretexting (de l'anglais « pretext », en français : prétexte) :
L'attaquant vise à obtenir l'accès à des données sensibles ou à des systèmes protégés. Il commence par instaurer la confiance en se présentant comme une personne digne de confiance et en imaginant une histoire bien ficelée. L'agresseur se fait passer pour un collaborateur d'une grande entreprise, un policier ou un employé de banque, par exemple. Il peut poser des questions soi-disant nécessaires pour confirmer l'identité de la victime, mais il s'agit en fait de collecter un maximum de données et d'informations sur la victime (p. ex. des informations internes à l'entreprise, des données personnelles, des documents bancaires ou des informations sur la sécurité). Attention : cela peut également se produire lors d'un contact direct avec une personne, et pas seulement en ligne, par e-mail ou par téléphone.

Fraude au CEO :
Tu reçois un e-mail apparemment légitime de ton chef (CEO, de l'anglais « Chief Executive Officer »), dans lequel on te demande d'effectuer une mission pour lui ou de lui rendre un service. Dans l'e-mail, la personne se présente spécialement comme une personne d'autorité (précisément comme le chef d'entreprise/le CEO). Les gens ont tendance à exécuter plus facilement une mission qui leur est confiée par une personne d'autorité/de respect, même s'ils enfreignent les règles ou agissent contre leur propre volonté. Lorsque la pression du temps est forte et que l'urgence est clairement indiquée, la pensée rationnelle est encore plus négligée. Ceci avant tout : ne réponds jamais à un tel e-mail, ne clique pas sur le lien qu'il contient et n'ouvre pas la pièce jointe au mail !

Mesures de protection contre le social engineering

Les « social engineers » exploitent les caractéristiques humaines et non les faiblesses techniques. Une entreprise peut donc disposer d'une infrastructure informatique (réseau, serveurs) entièrement et parfaitement sécurisée, mais les escrocs parviennent tout de même à accéder aux données de ses clients.

Comment peux-tu alors te protéger contre l'ingénierie sociale ?

- Examine de manière critique toutes les prises de contact et tous les messages (e-mail, appels, SMS) ! Il est bien possible que tu connaisses le nom de l'expéditeur ou de l'expéditrice. Dans ce

cas, vérifie bien l'adresse e-mail et le numéro de téléphone ! L'e-mail provient-il vraiment de la personne que tu penses connaître ? Ou est-ce qu'une adresse e-mail étrange se cache dans le champ de l'expéditeur ?
- Ne communique jamais tes données d'accès (mots de passe, numéros de contrat, code de sécurité) et veille à ce que personne ne te regarde taper un mot de passe !
- Ne clique jamais sur les liens des e-mails ou des SMS qui te semblent suspects ! N'ouvre pas les pièces jointes !
- Si tu es invité à effectuer un paiement par e-mail ou par SMS, vérifie soigneusement la demande avec le destinataire et contacte-le au numéro de téléphone officiel !
- Veille à ce que tes appareils et tes logiciels soient toujours à jour !
- Choisis des mots de passe sûrs !
- Fais des copies de sauvegarde / back-ups de tes fichiers importants !
- Ne visite que des sites web dignes de confiance ! Si « https:// » figure devant l'adresse web (URL), il s'agit plutôt d'un site sécurisé.
- Fais attention à ces lignes d'objet d'e-mails et à d'autres similaires : « Vérification du mot de passe requise immédiatement », « Problème avec votre compte bancaire », « Dernier rappel : veuillez répondre immédiatement », « Votre commande sur Amazon.com ». Il est fort possible que ces e-mails te parviennent en anglais. Sois d'autant plus prudent avec les lignes d'objet telles que « Urgent request », etc.

Sources

Etzemüller, Thomas (2017) : Social engineering, version : 2.0, dans : Docupedia-Zeitgeschichte, http://docupedia.de/zg/Etzemueller_social_engineering_v2_de_2017, DOI : https://doi.org/10.14765/zzf.dok.2.1112.v2, [22.11.22].

Fox, Dirk (2014) : Social Engineering im Online-Banking und E-Commerce, dans : Datenschutz und Datensicherheit - DuD 38, 325-328, https://link.springer.com/article/10.1007/s11623-014-0119-4, [22.11.22].

Meinert, Monica (2016) : Social engineering : the art of human hacking, dans : ABA Banking Journal, 108(3), 49-49.

Raiffeisen (2022) : Sécurité dans l'e-banking. Comment se protéger des fraudeurs, accessible en ligne : https://www.raiffeisen.ch/rch/de/privatkunden/e-banking/sicherheit-im-e-banking/verhaltenstipps.html, [22.11.22].

Tetri, Pekka et Vuorinen, Jukka (2013) : Dissecting Social Engineering, in : Behaviour & information technology 32.10, 1014-1023, DOI:10.1080/0144929X.2013.763860, [22.11.22].