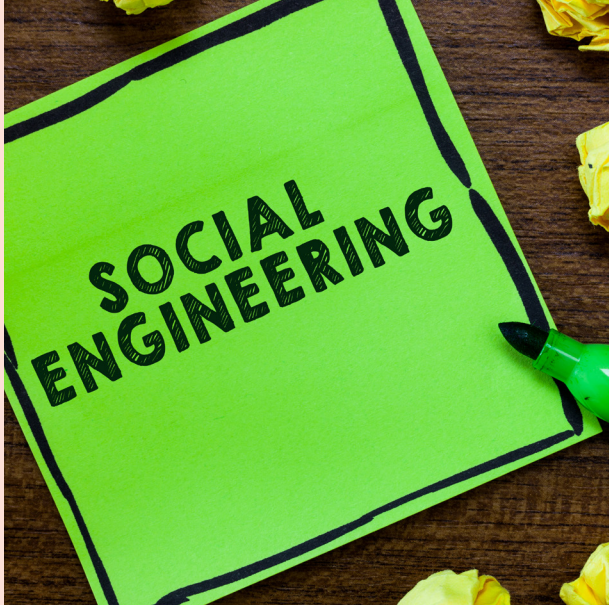
Fiche-conseils

LES ATTAQUES D'INGÉNIERIE SOCIALE

Souvent utilisée comme une reconnaissance de terrain, l'ingénierie sociale est aussi une méthode d'espionnage permettant d'obtenir des informations cruciales en exploitant la « faille humaine », la confiance, la crédulité ou l'ignorance de l'être humain. Qu'elle soit menée dans un but lucratif ou utilisée pour accéder à des systèmes ou à des informations jugées pertinentes, l'ingénierie sociale peut n'être qu'une première étape permettant à une personne malveillante de lancer des attaques informatiques précises et personnalisées.



L'art de la manipulation, du mensonge et de la tromperie

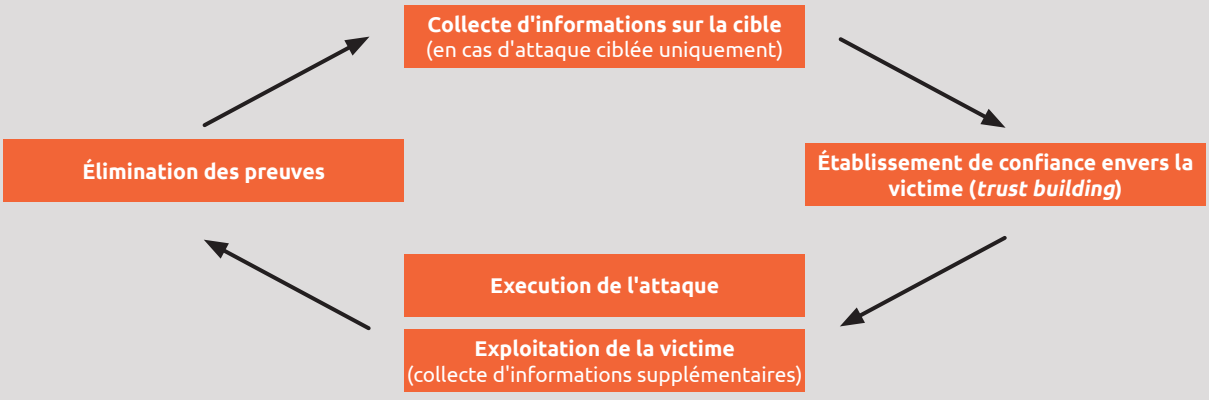
D'aussi loin que l'on puisse remonter dans le temps, l'ingénierie sociale a toujours existé. Arsène Lupin, le maître des voleurs, par exemple, avait recours à des astuces psychologiques et à la tromperie (*misdirection*) pour subtiliser des objets précieux. Plus largement, les magiciens trompaient, et trompent encore, leur public avec des illusions rondement menées pour prouver que la magie existe vraiment.

L'ingénierie sociale implique ainsi des compétences de manipulation et de mensonge pour persuader une victime de sa bonne foi et ainsi gagner sa confiance. Au-delà de la manipulation de la communication, elle implique des effets psychologiques tels que le langage corporel ou le ton de la voix.

Les attaques d'ingénierie sociale exploitent une faiblesse des fonctions cognitives de l'être humain, grâce, notamment, aux processus d'influence, de manipulation, d'incitation et de faux-semblants.

Sur le plan informatique, ces attaques se traduisent, par exemple, par des tentatives d'hameçonnage (*phishing*), d'hameçonnage vocal (*voice phishing* ou *vishing*) ou bien encore de prétexte (*pretexting*), pour ne citer qu'eux. Elles peuvent se montrer aussi redoutables que le piratage classique alors même que la personne malveillante à la base de l'attaque dispose de moins de connaissances techniques.

Cycle de vie d'une attaque d'ingénierie sociale



© Copyright Fondation Restena - Octobre 2021 | www.restena.lu

restena
réseau · sécurité · .lu

Principales techniques de collecte d'informations

Fouille de déchets

Les poubelles et conteneurs à déchets peuvent contenir de véritables trésors : plans d'architectures, documents confidentiels non-détruits, post-its griffés d'informations importantes.

Recherche d'accès mal protégés

Des bâtiments mal protégés, des portes non fermées à clef ou mal fermées sont des accès faciles… tout comme tenir la porte à une personne que l'on ne connaît pas en entrant dans un bâtiment ou une zone disposant d'un accès sécurisé, par lecteur de badges notamment.

Manipulation de personnes

Les médias (réseaux sociaux, annuaires d'entreprises, sites Internet, etc.) diffusent de nombreuses informations sur les entreprises et leurs employés. Une fois ces données en sa possession, l'attaquant va s'en servir pour se crédibiliser auprès de sa victime ou soutirer à son interlocuteur des informations encore plus précises.

Principaux scénarios d'attaques

Grâce aux informations collectées, les personnes malveillantes sont capables de lancer de multiples scénarios d'attaques qui ne se réduisent pas seulement à l'utilisation des outils informatiques.

Le saviez-vous ?

84% des attaques cyber ont une origine d'ingénierie sociale*

Hameçonnage (vocal) - *phishing* (*vishing*)

Par le biais d'un message écrit ou d'un contact téléphonique, l'attaquant tente de récupérer les informations privées (carte de crédit, mot de passe, adresse physique, email, etc.) de sa victime en se faisant passer pour quelqu'un qu'il n'est pas.

Fraude au président (*CEO fraud*)

L'attaquant demande à sa victime de transférer une somme d'argent en se faisant passer pour un membre de la direction ou une personne bien placée dans l'organisation. Cette fraude a recours à différentes techniques : le harponnage (*spear phishing*), la chasse (*whaling*), ou le *deepfake*.

Vol de données en physique

L'attaquant exfiltre les données confidentielles d'une organisation et les rend publiques et/ou accessibles à des personnes non autorisées.

Installation de systèmes de capteurs malveillants

Variante 1 : attaque logicielle

L'attaquant convainc sa victime d'installer, directement sur son matériel (ordinateur, smartphone, machine à café, etc.), un programme, un logiciel ou tout autre capteur malveillant – tel qu'un enregistreur de frappe (*keylogger*) – sans qu'elle ait conscience de la mauvaise utilisation qui en sera faite.

Variante 2 : attaque physique

L'attaquant se rend physiquement sur site en utilisant des accès mal protégés (portes ouvertes ou déguisement) pour installer dans des lieux stratégiques avec accès restreints (tels que des machines dans un centre de calculs), des *keyloggers* ou autres capteurs de surveillance.

L'ingénierie sociale cible le maillon le plus faible de la chaîne : l'être humain.

** Source : Agence européenne pour la cybersécurité - European Union Agency for Cybersecurity (ENISA), rapport : 'Cybersecurity for SMEs - Challenges and Recommendations', juin 2021*

© Copyright Fondation Restena - Octobre 2021 | www.restena.lu

Éviter une attaque d'ingénierie sociale

De manière générale, pour se prémunir de l'ingénierie sociale, la vigilance et l'esprit critique sont indispensables. La prévention et la sensibilisation de l'ensemble des employés par les équipes informatiques voire l'équipe Computer Security Incident Response Team (CSIRT) si existante, restent la meilleure défense.

- **Conservez sous clef et protégez par mot de passe l'ensemble des informations confidentielles :** que ces informations vous concernent personnellement ou non, ou qu'elles aient trait à des détails de l'activité de votre institution ou de ses partenaires, ne les laissez pas accessibles.
- **Ne transmettez aucune information confidentielle sans vous être assurés au préalable de l'identité du demandeur,** et ce indépendamment du canal de communication utilisé.
- **Ne vous laissez pas 'charmer' par des paroles flatteuses ni intimider par des propos menaçants :** si les paroles que vous entendez vous semblent excessives, méfiez-vous !
- **Informez-vous régulièrement sur les protocoles et procédures de sécurité qui ont cours au sein de votre institution :** plus vous serez informés, plus vous pourrez connaître les limites à ne pas franchir pour garantir votre sécurité, celle de vos collègues et celle de votre institution.

Réagir face à une attaque d'ingénierie sociale

Au moindre doute, même le plus infime, sur la véracité d'un mail, d'une demande d'information, ou bien encore sur l'existence d'une personne, réagissez immédiatement.

- **Validez la demande d'informations par un autre canal d'information :** discutez avec vos collègues, entretenez-vous sur le contenu de la demande avec votre hiérarchie.
- **Demandez à la personne en question de vous contacter par un autre biais :** grâce à cela, vous pourrez vous assurer de son identité, voire même de son existence réelle.
- **Posez des questions supplémentaires pour détecter d'éventuelles anomalies lors de la conversation :** demandez à votre interlocuteur des précisions sur des choses qu'il est censé connaître ou poursuivez la conversation avec des informations volontairement erronées pour juger de sa réaction.
- **Coopérez avec le service informatique ou l'équipe CSIRT de votre institution :** même si aucune action précise ne peut être prise à l'encontre de la personne malveillante qui est entrée en contact avec vous, le service doit à minima être informé de l'existence de ce fléau. Charge à lui, par la suite, de prendre les mesures nécessaires sur son infrastructure technique et surtout d'informer et sensibiliser l'ensemble des employés.
- **Demandez un badge visiteur ou son identité à une personne que vous rencontrez dans un lieu restreint /protégé et que vous ne connaissez pas :** la sécurité physique joue un rôle primordial, n'hésitez pas, au pire, à accompagner la personne vers le poste de sécurité ou à informer le poste de sécurité.

Dans l'ingénierie sociale, les attaquants procèdent à la manière 'agir avant de réfléchir' ('act before you think') très souvent en mettant la pression sur la victime ou en simulant une urgence. La meilleure façon de se protéger est donc toujours de 'réfléchir avant d'agir' ('think before you act').

'Social engineering bypasses all technologies, including firewalls'
citation de Kevin Mitnick, auteur de plusieurs livres sur la cybersécurité

© Copyright Fondation Restena - Octobre 2021 | www.restena.lu

Recommandations et responsabilité

Détruisez de manière définitive tout document et matériel informatique contenant des informations confidentielles dont vous n'avez plus besoin.

Déchiquetez les documents imprimés et démagnétisez vos disques durs à l'aide d'outils adaptés.

Sécurisez l'accès à tout matériel, équipement ou bâtiment.

Sécurisez vos accès avec des mots de passe efficaces et à jour, maintenez vos bases de données à jour, cryptez les équipements informatiques si nécessaire, etc.

Ne faites pas aveuglément confiance aux demandes de personnes que vous ne connaissez pas.

Restez alerte, remettez en question le bien-fondé des requêtes que vous recevez, et ce par quelque biais que ce soit.

Exemple : La vulnérabilité de la recherche et l'éducation

Il est assez facile pour un attaquant de se faire passer pour un étudiant et de poser des questions en rapport avec le cours ou bien encore de s'inscrire sur des listes de mails destinées à des étudiants et de là obtenir des informations sur les personnes du groupe.

Les informations obtenues, l'attaquant pourra tenter de bloquer des données essentielles pour l'institution, dévier l'argent des budgets de subventions destinés à des projets de recherche et développement ou encore accéder à des questions d'examens qu'il pourra alors soit utiliser à ses propres fins, soit revendre à des tiers.

Offre de services

Grâce à son équipe de réponse aux incidents de sécurité informatique (Restena-CSIRT), la Fondation Restena aide la communauté luxembourgeoise de la recherche et de l'éducation confrontée à des incidents de sécurité informatique. Elle réalise également des campagnes de phishing et de sensibilisation sur mesure sur des sujets d'actualité, et co-organise des conférences, telles que CyberDay.lu et Data Privacy Day.

Pour plus d'informations sur ce service, rendez-vous sur restena.lu/CSIRT

© Copyright Fondation Restena - Octobre 2021 | www.restena.lu

restena
réseau · sécurité · .lu