Région de gendarmerie Nouvelle-Aquitaine
Antenne Sécurité Économique et Protection des Entreprises de la formation administrative de Poitou-Charentes
Groupement de gendarmerie départementale de la Vienne.

INGENIERIE SOCIALE

Ingénierie sociale: Approche systémique et psychologique, facilitée par une manœuvre dolosive d'une personne mal intentionnée qui recueille, à leur insu, des informations précises sur une entreprise ou un particulier.

DE QUOI PARLE T-ON ?

Croire qu'un pirate informatique élabore son attaque par la seule voie logicielle est erroné.
En effet, toute faille constitue pour le hacker un moyen d'atteindre son objectif. L'ingénierie sociale, dénommée également "faille humaine", en est une composante essentielle.
Les réseaux sociaux servent en partie ces informations sur la place publique virtuelle. Il est aussi possible de se les procurer directement et plus simplement en téléphonant à la future victime ! Les escrocs, réalisant de tels actes, excellent dans cet art.

Explications :

L'ingénierie sociale est un " art négatif " réalisé pour parvenir à des objectifs illégitimes, en contournant les différentes sécurités physique et informatique existantes. Il devient alors possible de recueillir des informations sensibles. La finalité est multiple : Pénétrer un système ; détourner, voler ou détruire des informations ; escroquer une société ou une personne. Les « prédateurs » font preuve de persuasion en exploitant la naïveté et le stress de leur « proie » ainsi que d'une parfaite maîtrise des techniques de manipulation qui met inévitablement la victime dans un état d'acceptation de la demande.
Les arnaques d'ingénierie sociale se réalisent souvent suivant le modus operandi ci-dessous :
❶ Mise en confiance du correspondant. Se faire passer pour un chef hiérarchique en est l'illustration la plus fréquente. Technique utilisée dans les Faux Ordres De Virements Internationaux FOVI.
❷ Déstabilisation de l'interlocuteur par une mise en alerte et une demande impérieuse.
❸ Rassurer le correspondant et le forcer à limiter sa focalisation sur l'alerte donnée précédemment.
Pour rappel, ces attaques se font par courrier, par courriel et par téléphone.
A titre d'exemple, récemment, un anonyme s'est fait passer pour un dépanneur en télémaintenance de Microsoft auprès d'une société en usant de l'ingénierie sociale. Cela lui a permis de prendre la main sur l'ordinateur de la personne contactée et d'y installer un Scareware, faux logiciel de sécurité qui simule des alertes de sécurité. Il a ainsi créé un état d'anxiété chez l'utilisateur pour l'amener à « obéir » aux différentes mesures préconisées par le logiciel.
Enfin, le danger potentiel est également l'utilisation de cet ordinateur pour procéder à des attaques de déni de service ou pour installer des rançongiciels et autres programmes malins.

Précautions :

Une vigilance de tous les instants est la solution idoine pour maîtriser les risques de cette nature et les prévenir.
D'autres permettent de limiter fortement ces tentatives d'ingénierie sociale :
- Ne pas diffuser d'informations stratégiques ou sensibles de votre entreprise sur les réseaux sociaux ;
- Se méfier des amis qui vous « veulent du bien » sur les réseaux sociaux ;
- Les mots de passe privés ne doivent pas être identiques à ceux utilisés au travail ;
- Se renseigner sur l'identité du correspondant et lui proposer de réaliser un contre-appel ;
- Réaliser des séances de sensibilisation ;
- Former les remplaçants ;
- Se méfier des attaques pendant les périodes de congés ou en fin de semaine.

Réactions :

Chacun doit être conscient de la sophistication des fraudes permise par l'ingénierie sociale.
Lorsque vous pensez avoir fait l'objet d'une attaque de type ingénierie sociale, il est souhaitable de :
- Vérifiez auprès de votre banque si des transactions illicites ont été passées sans votre accord (FOVI) ;
- Faites un audit de sécurité de votre système informatique ;
- Sensibilisez vos personnels.

AU MOINDRE DOUTE, ALERTEZ IMMÉDIATEMENT LES FORCES DE L'ORDRE