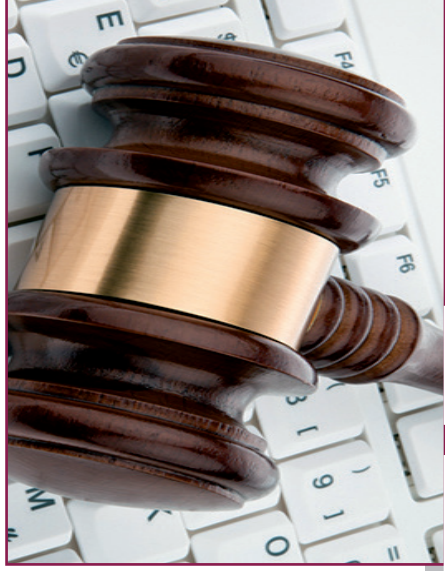
9

L'ingénierie sociale

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

L'ingénierie sociale



Basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs, cette technique permet de soutirer de l'information aux victimes sans avoir recours à l'outil informatique, mais à des moyens de communication plus "traditionnels" tels le téléphone, le courrier écrit, la messagerie instantanée et parfois même le contact direct. Plus intéressant encore, les pirates d'aujourd'hui exploitent l'abondance d'informations personnelles disponibles sur les sites de réseaux sociaux pour cibler leurs attaques sur les individus clés au sein des entreprises visées.
L'ingénierie sociale est l'une des menaces les plus anciennes et les plus sérieuses pour les réseaux informatiques sécurisés. C'est un type d'attaque très performant dans la mesure où aucun logiciel ni matériel ne permet de s'en défendre efficacement.

D'une manière générale les méthodes d'ingénierie sociale se déroulent selon le schéma suivant :

- Une phase d'approche permettant de mettre l'utilisateur en confiance, en se faisant passer pour une personne de sa hiérarchie, de l'entreprise, de son entourage, d'un fournisseur, etc.

- Une mise en alerte, afin de le déstabiliser. Il peut s'agir par exemple d'un prétexte de sécurité ou d'une situation d'urgence ;

- Une diversion, c'est-à-dire une phrase ou une situation permettant de rassurer l'utilisateur et d'éviter qu'il se focalise sur l'alerte. Il peut s'agir par exemple d'un remerciement annonçant que tout est rentré dans l'ordre, d'une phrase anodine ou dans le cas d'un courrier électronique ou d'un site web, d'une redirection vers le site web légitime.

Comment se protéger ?

La meilleure façon de se protéger est d'utiliser son bon sens pour ne pas divulguer à n'importe qui des informations pouvant nuire à la vie privée ou à la sécurité de l'entreprise. Il est ainsi conseillé, quel que soit le type de renseignement demandé :

- De se renseigner sur l'identité de son interlocuteur en lui demandant des informations précises (nom et prénom, société, numéro de téléphone) ;
- De vérifier éventuellement les renseignements fournis ;
- De s'interroger sur la criticité des informations demandées.