Social Engineering

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Cette fiche présente les techniques d'attaques regroupées sous le nom de « social engineering ». Elle décrit comment les attaquants parviennent à avoir accès à des ressources confidentielles par la manipulation de personnes de bonne foi qui, elles, y ont légitimement accès.

Table des matières

1 Qu'est-ce-que le social engineering ?

C'est une technique de manipulation par tromperie qui vise à obtenir l'accès à des informations confidentielles ou à des ressources à accès restreint par la manipulation de personnes en ayant directement ou indirectement l'accès. Le « phishing » est une application particulière de ce type d'attaque.

Le social engineering ne s'applique pas seulement au domaine de l'informatique, il peut être rencontré dans la vie de tous les jours et plus particulièrement sur le lieu de travail. À partir du moment où des ressources ayant un certain intérêt sont en jeu, des attaques de ce type peuvent apparaître. De ce fait, les grandes organisations sont des cibles souvent plus faciles en raison de la dispersion de l'information et du personnel.

Ainsi, le facteur humain est le point central des techniques d'attaque rencontrées en social engineering. Des relations de confiance ne reposant sur rien de concret sont mises en place de manière calculée mais le plus souvent par simple discussion, et exploitées par la suite pour tirer un maximum de profit de la situation.

2 Comment cela fonctionne-t'il ?

Les techniques de social engineering exploitent certaines failles dans le comportement humain et dans la manière dont sont organisées les entreprises. Il est en effet dans la nature humaine de vouloir aider son prochain et d'accorder sa confiance aux personnes polies et d'abord sympathiques, même si celles-ci sont des inconnus. Tout dépend de la situation et de la manière utilisée par le ou les attaquants pour se présenter. Bien souvent, une simple demande directe peut suffire.

Le but de l'attaque vise à faire exécuter à une personne une action qu'elle n'aurait pas faite en temps normal ; la motivation de l'attaquant étant d'obtenir une information qu'il ne contrôle pas. Dans un monde de plus en plus informatisé, ceci se résume le plus souvent (mais ne se limite pas), à l'obtention de données d'authentification.

Un attaquant peut, par exemple, tenter en premier lieu d'établir une relation de confiance avec un membre du avec qui il va passer un certain temps à rechercher des informations sur l'entreprise visée. Il n'est donc pas rare de rencontrer des attaquants ayant une connaissance approfondie du jargon employé dans le métier de l'entreprise et des procédures mises en place par celle-ci. En effet, ceci facilite les prises de contact en interne et permet de faire passer plus aisément des requêtes qui, sinon, pourraient paraître suspectes.

Social Engineering

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Du point de vue de l'employé, celui-ci se trouve face à une personne qui semble averti des procédures internes et qui utilisant un jargon commun. Dans une grande entreprise oú tout le monde ne peut se connaître, l'employé n'a pas de raison d'être soupçonneux et coopère. Pensant bien faire son travail en proposant son aide à ce qu'il pense être un collègue, il n'a pas de raison de refuser. Bien souvent, les réflexions liées à la sécurité viennent après l'action et, à ce moment là, l'attaquant a déjà disparu sans laisser de traces, avec de précieuses informations en sa possession. .
Dans ce cas-ci, on est face à un attaquant bien informé et qui va droit au but.

D'autres approches sont également possibles, notamment en ce qui concerne la récupération d'informations. L'attaquant peut se présenter comme chargée d'enquêter sur le domaine d'activité de la cible. Il pose alors toute une série de questions anodines parmi lesquelles se cache celle dont la réponse l'intéresse tout particulièrement. Cela peut, par exemple, être une question sur le jargon de l'entreprise ou sur une convention particulière employée par celle-ci (une convention de nommage des produits par exemple).

L'attaquant peut adopter une stratégie tout à fait différente en engendrant une situation problématique pour sa victime, puis se présenter ensuite à elle comme étant la personne qui peut l'aider à en sortir. Dans la plupart des cas, la victime se montrera coopérative et répondra sans broncher aux questions les plus précises de l'attaquant.

3 Qui est concerné ?

Les cibles de telles attaques sont très variées, allant du simple particulier à de grandes entreprises. L'utilisation de moyens informatiques ou l'accès à l'Internet ne sont pas des pré-requis pour être victime d'un acte de social engineering. L'avènement des nouvelles technologies offre simplement de nouveaux vecteurs d'attaques ; le contact direct, le téléphone ou même le courrier postal classique sont aussi employés.

Les clients d'une société peuvent également présenter un intérêt aux yeux d'un attaquant. Dans ce cas, la société concernée est utilisée elle-même comme vecteur pour atteindre les clients et les ressources auxquelles elle a accès de plein droit.

4 Exemple : les « scammers »

Le terme « scammers » regroupe les individus tentant d'escroquer d'autres personnes par l'envoi de mails sollicitant de l'aide pour placer des quantités d'argent très importantes, hors d'atteinte des autorités. Pour allécher sa victime, le scammer lui propose de placer une somme sur son propre compte bancaire. Pour renforcer l'impression d'authenticité de la demande, le scammer n'hésite pas à se prétendre lié à une agence gouvernementale quelconque et fait usage de documents apparemment authentiques.

Voici un exemple d'email provenant d'un scammer :
From: <christelle.eyadema@jumpy.it>
Sent: Friday, 01 April, 2005 2:43
Subject: confidentialité

"J'ai l'honneur de venir par le biais de ma lettre vous informer mon désir ardent d'entamer une relation d'affaire avec vous.
Je m'appelle Christelle EYADEMA, je suis la fille du Président Gnassingbé EYADEMA née d'une mère Ivoirienne... "

Le but du scammer est de réussir à soutirer de l'argent à sa victime. Pour ce faire, il va justifier des frais divers afin de pouvoir effectuer le transfert censé apporter à chacun un gain financier conséquent.

5 Recommandations

5.1 Comment le détecter ?

Les attaques par social engineering ne sont pas nécessairement complexes. Il arrive qu'elles se résument à une simple demande d'information directe et anodine. Une attaque peut avoir pour objectif d'obtenir des renseignements préalables à une future attaque sur une autre cible. Toute demande d'information précise sur des procédures, des habitudes ou des précisions sur du vocabulaire interne provenant d'une personne inconnue et extérieure au milieu de travail peut être considérée comme suspecte.

Social Engineering

5.2 Comment s'en prémunir ?

Toute information, même paraissant insignifiante, doit être considérée comme importante. Il est nécessaire de sensibiliser les employés à ce type de problèmes car chacun d'eux est susceptible de manipuler des informations potentiellement intéressantes pour un attaquant.

Si une politique de sécurité est définie dans l'entreprise, les procédures qui y sont décrites doivent être strictement suivies. Ceci est particulièrement vrai pour les employés récemment arrivés, peu habitués à leur nouvel environnement de travail et qui constituent de ce fait des cibles privilégiées. De plus, il est essentiel que le suivi de la politique de sécurité s'applique également aux employés n'ayant pas accès à l'outil informatique.

Il faut rester conscient que la connaissance du jargon, des procédures et des habitudes de l'entreprise ne fait pas d'un inconnu, une personne de confiance. En cas de doute il est préférable de procéder à une vérification d'identité. Au téléphone, il est recommandé de demander à l'interlocuteur son numéro de poste et après vérification de celui-ci, de le rappeler. Cette vérification consiste à s'assurer que la personne à qui l'on parle, dispose d'un accès légitime au poste téléphonique d'où elle appelle.

Dans le monde informatique, il existe quelques règles simples qui permettent de garantir un minimum de protection face au social engineering. Ce sont principalement des règles de bon sens, utilisables aussi bien sur le lieu de travail que devant l'ordinateur familial.

Ainsi, il faut protéger au maximum ses mots de passe et surtout ne jamais les divulguer. Pour cela, il faut absolument éviter d'utiliser des commandes non-familières dictées par un inconnu.

Il faut éviter d'ouvrir tout fichier attaché à un mail provenant d'une source douteuse ou même tout fichier provenant de sites Internet douteux. Bien souvent, ce genre de fichier semble de prime abord, anodin et inactif. En revanche, en arrière plan, la destruction des documents de l'utilisateur, l'envoi de ceux-ci sur un site Internet contrôlé par un attaquant, voire même la prise de contrôle de la machine à distance sont possibles.

Une dernière recommandation concerne les documents imprimés sur papier. Evitez de laisser de telles sources d'information à la portée de tous. (Ceci est également vrai pour les documents mis à la poubelle). Il est donc recommandé de les rendre inintelligibles en les brûlant ou en les déchirant avant de les jeter.

CASES,
pour plus de sécurité dans l'utilisation des systèmes d'information électroniques. Une initiative européenne soutenue par l'Etat luxembourgeois

OFFICE LUXEMBOURGEOIS D'ACCREDITATION ET DE SURVEILLANCE

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Economie et du Commerce extérieur