

Ingénierie Sociale

Retour sur une vulnérabilité critique: l'utilisateur lambda

Le mythe du « hacker dans son garage » a progressivement laissé place à la réalité des organisations spécialisées dans la cybercriminalité. Aussi nous constatons aujourd'hui que les attaques informatiques sont de plus en plus tournées vers les données, les applications et... les utilisateurs. S'il existe des moyens techniques pour sécuriser les applications et les réseaux, force est de constater qu'il reste beaucoup à faire sur le plan de l'humain.vulnérable, plus il sera sensible aux menaces et plus les conséquences seront importantes. C'est logique et malheureusement constaté.

L'utilisateur: Maillon faible de la sécurité

Pour pénétrer un système informatique, on passait généralement « par la grande porte » : recherche du Buffer Overflow ultime, exploitation d'une faille tricky, ... mais pourquoi passer par la porte fermée si la fenêtre est laissée ouverte?

Pourquoi perdre son temps en tentative d'intrusion (brute force, techniques d'évasion, adaptation d'exploits, ...) sur un service alors qu'il suffit de contacter l'utilisateur pour obtenir ses identifiants de connexion?

Il n'est pas nécessaire de passer 3 heures à adapter un Shell code quand on a la possibilité d'obtenir les données nécessaires en 3 minutes au téléphone avec un utilisateur.

Démonstration...

Intrusion sur un réseau non accessible depuis Internet

Mardi 6 octobre 9h27. Denis S. se présente à l'accueil du siège social d'une société connectée à Internet par un simple routeur ADSL, sans accès entrant possible:

Denis: « Bonjour madame, j'ai trouvé cette clé usb sur le trottoir. Le nom de votre société y étant inscrit, je me suis permis de vous l'apporter ».

Accueil: « Oh ! Merci monsieur, c'est très gentil ».

Denis: « Je vous en prie, bonne journée ».

La clé usb remise contenait quelques fichiers vides... ainsi qu'un cheval de Troie qui s'exécute automatiquement dès l'insertion de la clé sur le poste.

Ce programme malveillant se connecte ensuite sur un site sous contrôle de Denis qui peut alors initier une connexion VNC vers le poste de la victime.

Mardi 6 octobre 10h12. Denis S est de retour au bureau... et a le contrôle total du poste du directeur administratif et financier de cette société :



Technique d'évasion avancée: Contournement d'un VPN-SSL à 20k€ en 3 minutes

De la même manière, il est tout aussi facile de pénétrer un système donc l'accès est correctement sécurisé.

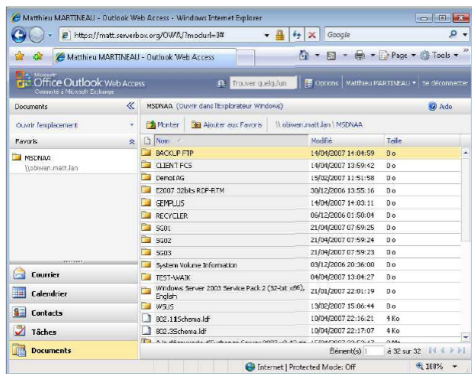
L'apogée du Web 2.0, du « Web Social », permet une optimisation non négligeable de la première phase des attaques par ingénierie sociale: la recherche d'informations. En quelques clics, nous obtenons informations personnelles et professionnelles sur les collaborateurs de la société cible.

Le scénario d'attaque n'a ensuite pour seule limite que l'imagination de l'attaquant.

En prétextant opérations de maintenance, ou vérifications du bon fonctionnement du compte, nous

parvenons sans mal à diriger l'utilisateur vers un portail pour y saisir ses identifiants de connexion...

Au bout de quelques minutes, nous sommes en possession d'un compte utilisateur valide pour se connecter au VPN de la société :



Cette attaque nous aura permis de contourner un VPN-SSL et les moyens mis en oeuvre pour sécuriser le webmail en quelques minutes... sans avoir à mettre les mains dans la technique.

Une menace sous estimée

Les exemples illustrés précédemment sont issus de cas réels. Les techniques d'ingénierie sociale reposent sur les faiblesses humaines, elles suivent un schéma basé sur une analyse du comportement des interlocuteurs. Par manque de sensibilisation de ces derniers le taux de réussite de ce type d'attaque est alarmant.

Dans l'objectif de rechercher ou d'atteindre la donnée, les applications et les utilisateurs sont en première ligne des attaques. Plus de 70% des attaques visent les applications Web sur Internet. Le phishing, le Carding, le pharming sont autant de pratiques nouvelles destinées à collecter en masse des informations personnelles (numéros de cartes bleues, numéros de comptes, ...) qui sont revendues par la suite sur Internet.

Il suffit aujourd'hui d'une simple connexion sur un

site sous contrôle d'une personne malveillante pour réussir à piéger un utilisateur. On exploite ensuite les faiblesses des postes de travail, navigateurs ou composants non maintenus à jour (plugins PDF, flash, ...). Ainsi, les attaques par phishing, faciles à détecter et généralement grossières, laissent de plus en plus place à l'exploitation de failles XSS beaucoup plus subtiles (téléchargement de fichiers PDF compromis par exemple).

Fatal Exception Error (0xxx): Common sense is missing...

En dépit de la montée en puissance de l'ingénierie sociale, ces attaques sont aujourd'hui encore sousestimées.

A l'heure où le web 2.0 est plus que jamais présent, où les entreprises encouragent même leurs collaborateurs à utiliser et à communiquer via les réseaux sociaux (Viadeo, Facebook...), il n'a jamais été aussi simple de réunir des informations sur les collaborateurs et partenaires d'une société.

Ce qui est d'autant plus préoccupant quand on s'intéresse aux techniques employées par les organisations malveillantes. La finalité de leurs attaques est davantage tournée vers l'espionnage industriel, le commerce des données collectées, ...

Il n'y a pas de limites dans les moyens mis en oeuvre pour obtenir ces informations (ex: Embauche d'un collaborateur pour s'introduire dans la société). Dans un tel contexte, une organisation n'hésitera pas à consacrer plusieurs mois pour parvenir à ses fins.

Et pourtant, de simples règles de bon sens et de respect des bonnes pratiques de sécurité permettraient de se prémunir contre ce type de failles... : une surveillance et un contrôle stricts des accès, une organisation de la sécurité, l'application des mises à jour et correctifs de sécurités sur les systèmes, une classification des données sensibles... et surtout : Une sensibilisation des utilisateurs. ■

A propos d'Advens

Advens est une société de conseil spécialisée en management de la sécurité de l'information.

Depuis plus de 10 ans, nous aidons les organisations à piloter la sécurité de l'information en parfait alignement avec leurs enjeux métier et pour en améliorer la performance.

Une approche unique qui repose sur une expertise sectorielle pointue dans les domaines de la distribution, de la finance, de l'industrie, de la santé, des services ou de l'administration publique et aide les RSSI à construire une fonction sécurité efficace et valorisée.

Avec des bureaux à Lille et à Paris et une équipe de spécialistes expérimentés, Advens compte parmi ses clients des entreprises leader sur leur marché telles qu'Arcelor Technologies, Auchan, le Groupe Crédit Agricole, Cofidis, Decathlon, Eurotunnel, la Société des Paris Sportifs ou encore le Ministère de l'Education Nationale.

PARIS

5, rue du Helder, 75009 Paris
Tel : +33 (0)1 53 24 00 70
Fax : +33 (0)1 53 24 53 39

LILLE

47, rue du Faubourg de Roubaix
Lille Europe - 59000 Lille
Tel : +33 (0)3 20 68 41 81
Fax : +33 (0)3 20 70 54 28

www.advens.fr
