Sujet: l’Ingénierie Social (social engineering)

L'ingénierie sociale est une technique de plus en plus courante pour les cybercriminels, car elle est souvent plus facile à mettre en œuvre que des techniques plus sophistiquées telles que les attaques par déni de service ou les logiciels malveillants. L'ingénierie sociale peut prendre différentes formes, telles que des appels téléphoniques, des e-mails ou des messages sur les réseaux sociaux.

Les cybercriminels peuvent se faire passer pour des personnes ou des organisations de confiance, telles que des employés de banque ou des représentants du gouvernement, pour obtenir des informations confidentielles telles que des mots de passe ou des numéros de carte de crédit. Ils peuvent également utiliser des techniques de persuasion pour inciter les victimes à exécuter des actions malveillantes, telles que l'installation d'un logiciel malveillant sur leur ordinateur.

Il est donc essentiel de sensibiliser les utilisateurs à l'ingénierie sociale et de leur apprendre à reconnaître les tentatives de manipulation. Les entreprises peuvent également mettre en place des politiques de sécurité strictes pour protéger les informations confidentielles.

Ma source principale pour cette veille est un article du site du magazine Le Point intitulé "Cybersécurité: comment l'ingénierie sociale menace votre entreprise". Cet article explique en détail les différentes techniques d'ingénierie sociale utilisées par les cybercriminels et donne des conseils pour se protéger contre ces attaques.

Source:
https://www.lepoint.fr/high-tech-internet/cybersecurite-comment-l-ingenierie-sociale-menace-votre-entreprise-01-10-2021-2450346_47.php