OUCH! Novembre 2020

Votre publication mensuelle de conscientisation à propos de la Sécurité

Attaques d'ingénierie sociale

Aperçu

Une fausse idée courante concernant les pirates informatique est qu'ils utilisent seulement des outils et techniques très sophistiqués pour pirater les ordinateurs et comptes des gens. Les pirates informatiques ont appris que les manières les plus simple pour voler votre information, pirater vos comptes ou infecter vos systèmes est en vous dupant pour le faire pour eux en utilisant une technique nommé l'ingénierie sociale. Apprenons comment ces attaques fonctionnent et ce que vous pouvez faire pour vous protéger.

Qu'est ce que l'ingénierie sociale

L'ingénierie sociale est une attaque psychologique ou l'attaquant vous dupe en vous faisant faire un geste que vous ne devriez pas faire au travers de diverses manipulations techniques. Pensez aux fraudeurs ou aux escrocs; c'est la même idée. Toutefois, les technologies d'aujourd'hui permettent aux pirates informatique de prétendre d'être n'importe quoi ou n'importe qui beaucoup plus facilement, peu importe leur emplacement dans le monde et cibler n'importe qui dans le monde, incluant vous. Jetons un coup d'œil à deux exemples concrets:

Vous recevez un appel téléphonique d'une personne prétendant être un représentant du gouvernement vous informant que votre paiement d'impôts est en retard et que, si vous ne payez pas votre due immédiatement, vous aurez une amende ou serrez arrêté. Ils vous font alors des pression pour effectuer un paiement immédiatement au téléphone avec votre carte de crédit, une carte cadeau ou un transfert bancaire, vous avertissant que si vous ne payez pas, vous pourriez aller en prison. L'appelant n'est pas vraiment du gouvernement, mais plutôt un attaquant qui tente de vous inciter à leur donner de l'argent.

Un autre exemple est un courriel nommé hameçonnage. C'est quand les attaquants créent un courriel qui tente de vous inciter à entreprendre une action, comme ouvrir une pièce jointe infectée, cliquer sur un lien malveillant ou encore donner des informations sensibles. Parfois, les courriels d'hameçonnages sont génériques et faciles à repérer, par exemple en faisant semblant de provenir d'une banque. D'autres fois, les courriels d'hameçonnages peuvent être hautement personnalisés et ciblés, car les attaquants recherchent d'abord leurs cibles, comme un e-mail d'hameçonnage prétendant provenir de votre patron ou collègue.

Gardez en tête que les attaques d'ingénierie sociale comme celles-ci ne se limitent pas aux appels téléphoniques ou aux courriels; ils peuvent se produire sous n'importe quelle forme, y compris par SMS, sur les réseaux sociaux ou même en personne. La clé est de savoir quels indices rechercher.

Indices communs d'une attaque d'ingénierie sociale

Heureusement, le bon sens est votre meilleure défense. Si quelque chose semble suspect ou ne semble pas correct, il peut s'agir d'une attaque. Les indices les plus courants comprennent:

- Un énorme sentiment d'urgence ou de crise. Les attaquants tentent de vous pousser à commettre une erreur. Plus le sentiment d'urgence est grand, il est plus probable qu'il s'agit d'une attaque.
- Pression pour contourner ou ignorer les politiques ou procédures de sécurité que vous devez suivre au travail.
- Les demandes d'informations sensibles auxquelles ils ne devraient pas avoir accès ou devraient déjà connaître, comme vos numéros de comptes.
- Un courriel ou un message d'un ami ou d'un collègue que vous connaissez, mais le message ne leur ressemble pas - peut-être que le libellé est étrange ou que la signature n'est pas correcte.
- Un courriel qui semble provenir d'un collègue ou d'une entreprise légitime, mais qui est envoyé à l'aide d'une adresse e-mail personnelle telle que @gmail.com.
- Jouer sur votre curiosité ou quelque chose de trop beau pour être vrai. Par exemple, vous êtes informé que votre colis a été retardé, même si vous n'avez jamais commandé de colis ou que vous avez gagné un prix dans un concours auquel vous n'avez jamais participé.

Si vous pensez que quelqu'un essaie de vous tromper ou de vous jouer un tour, ne communiquez plus avec cette personne. N'oubliez pas que le bon sens est votre meilleure défense.

Rédacteur invité

Christian Nicholson (@GuardianCosmos) est un instructeur SANS pour SANS SEC560 et SANS SEC504, ainsi que Partenaire/Cyber Lead chez Indelible(https://indelible.global). Christian est spécialisé dans la sécurité des applications, le Purple Teaming et l'automatisation pour une intégration, une programmation et une ingénierie sécurisées.

Ressources

Attaques par appel téléphonique: https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams
Arrêtez ce hameçonnage: https://www.sans.org/security-awareness-training/resources/stop-phish
PDG Fraude / BEC: https://www.sans.org/security-awareness-training/resources/ceo-fraudbec
Escroqueries Personalisées: https://www.sans.org/security-awareness-training/resources/personalized-scams

Traduit pour la communauté par: Jérôme Boutin et Sebastien Kierszka