OUCH! نوفمبر 2020

هجمات الهندسة الاجتماعية

نظرة عامة

من المفاهيم الشائعة و المغلوطة عن مهاجمى الفضاء الإلكروى أنهم يستخدمون فقط أدوات وتقنيات متقدمة للغاية لاخراق أجهزة الكمبيوتر أو حسابات الأشخاص. والحقيقة أن المهاجمس عبر الإنرنت قد تعلموا أن أسهل الطرق لسرقة معلوماتك أو اخراق حساباتك أو إصابة أنظمتك هى ببساطة خداعك لتقوم أنت بذلك نيابة عنهم، باستخدام تقنية تسمى الهندسة الاجتماعية. فلنتعرف على كيفية عمل هذه الهجمات وما الذي يمكنك القيام به لحماية نفسك.

ما هى الهندسة الاجتماعية

الهندسة الاجتماعية هى هجوم نفسى بحيث يخدعك المهاجم فيه للقيام بسىء لا يجب عليك فعله من خلال تقنيات التلاعب المختلفة. استحصر ما يفعله المخادعون أو المحتالون؛ إنها نفس الفكرة. ومع ذلك، فان التكنولوجيا هذه الأيام تسهل على أي مهاجم من أي مكان فى العالم، التظاهر بأنه أي سىء أو أي شخص يريده، واستهداف أي شخص فى أي مكان من العالم، بما فى ذلك أنت. دعونا نلقى نظرة على مثالس من العالم الحقيقى:

فأنت قد تتلقى مكالمة هاتفية من شخص يدعى أنه من الحكومة يخبرك بأن صرائبك متأخرة وأنك إذا لم تدفعها على الفور، فسيتم تغريمك أو توقيفك. ثم يضغطون عليك للدفع عبر الهاتف ببطاقة ائتمان أو بطاقة هدايا أو حوالة مصرفية محذرين من أنك إذا لم تدفع، فقد تذهب إلى السجن. المتصل هنا ليس من الحكومة حقا، ولكنه مهاجم يحاول خداعك لمنحهم المال.

مثال آخر هو هجوم بريد إلكروى يسمى بريد تصيد احتيالى. حيث ينسى المهاجمون بريدا إلكرونيا يحاول خداعك فيدفعك لاتخاذ إجراء ما، مثل فتح مرفق بريد إلكروى مصاب أو النقر فوق ارتباط ضار أو الافصاح عن معلومات حساسة. أحيانا تكون رسائل التصيد الاحتيالى عامة ويسهل اكتشافها، مثل التظاهر بأنها واردة من أحد البنوك. وفى أحيان أخرى، يمكن تخصيص رسائل البريد الإلكروى الاحتيالية و جعلها موجهة فى استهدافها بدرجة عالية، حيث يبحث المهاجمون عن أهدافهم أولا ،مثلا يرسلوا لك بريدا إلكرونيا احتياليا يبدو لك فعلا أنه قادم من رئيسك أو زميلك.

ضع فى اعتبارك أن هجمات الهندسة الاجتماعية كاللى سبق ذكرها لا تقتصر على المكالمات الهاتفية أو البريد الإلكروى؛ بل يمكن أن تحدث بأي شكل بما فى ذلك الرسائل النصية أو عبر وسائل التواصل الاجتماعى أو حى شخصيا .المفتاح لكشفها هو معرفة القرائن الى يجب البحث عنها.

القرائن المشركة لهجوم الهندسة الاجتماعية

لحسن الحظ فإن المنطق والفطره السليمة غالبا ما تكون أفضل دفاع لك. إذا كان هناك سيء يبدو مريبا أو لم يكن على ما يرام، فقد يكون هجوما. تشمل القرائن الأكثر شيوعا ما يلي:

- إيصال شعور هائل بالإلحاح أو الأزمة. يحاول المهاجمون دفعك لارتكاب خطأ. كلما زاد الشعور بالإلحاح، زاد احتمال وقوع هجوم.
- الضغط لتجاوز أو تجاهل السياسات أو الإجراءات الأمنية الى يتوقع منك اتباعها فى العمل.
- طلبات الحصول على معلومات حساسة لا ينبغى أن يكون لديهم إمكانية الوصول إليها أو لا يجب أن يعرفوها بالفعل كأرقام حسابك.
- رسالة بريد إلكترونى أو رسالة من صديق أو زميل فى العمل تعرفه، ولكن الرسالة لا تبدو مثله - قد تكون الصياغة غريبة أو توقيعه أسفل الرسالة غريبا أو غير صحيح.
- بريد إلكترونى يبدو أنه من زميل فى العمل أو سركة سرعية وأصلية، ولكن يتم إرسال البريد الإلكترونى باستخدام عنوان البريد الإلكترونى الشخصى مثل @ gmail.com.
- اللعب على إثارة فضولك أو لفتك لسيء من الجيد أن يبدو حقيقيا. على سبيل المثال، أن يتم إعلامك بانه تم تأخر توريد الطرد، على الرغم من أنك لم تطلب طردا مطلقا. أو أنك فزت بجائزة فى مسابقة لم تدخلها مطلقا.

إذا كنت تشك فى أن شخصا ما يحاول خداعك أو التحايل عليك، فلا تتواصل معه بعد الآن. تذكر,المنطق والفطرة السليمة غالبا ما تكون أفضل دفاع لك.

المحرر الضيف

كريستيان نيكلسون (GuardianCosmos) هو مدرس SANS لـ SANS SEC560 و SANS SEC504 ، بالإضافة إلى كونه سريك / قيادي فى(https://indelible.global). كريستيان متخصص فى أمان التطبيقات ، والتجمع الأرجوانى، والأتمتة للتكامل الآمن. والرمجة والهندسة.

الموارد

هجمات الاحتيال عبر الهاتف: https://www.sans.org/sites/default/files/2018-07/201807-OUCH-July-Arabic.pdf
لا تكن فريسة سهلة: https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Arabic.pdf
حيلة الرئيس التنفيذي: https://www.sans.org/sites/default/files/2018-09/201809-OUCH-September-Arabic.pdf
الحيل الشخصية: https://www.sans.org/sites/default/files/2019-02/201902-OUCH-February-Arabic.pdf

ترجمها للعربية: محمد سرور، فؤاد أبو عويمر، درويش الحلو، اسلام الكرد