أوتش! | نوفمبر (تشرين الثاني) ٢٠١٤

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- ما هي الهندسة الاجتماعية
- كيفية اكتشاف ووقف هجمات الهندسة الاجتماعية
- كيف تتفادى الهجمات المستقبلية

الهندسة الاجتماعية

ما هي الهندسة الاجتماعية

الهندسة الاجتماعية هي نوع من الهجوم النفسي حيث أن المهاجم يحاول خداعك حتى تقوم بتنفيذ ما يطلبه منك. الهندسة الاجتماعية موجودة منذ آلاف السنين، فكرة احتيال أو خداع شخص ليست جديدة. ومع ذلك، فقد تعلم المهاجمون أن استخدام هذه التقنية على شبكة الإنترنت فعالة للغاية ويمكن استخدامها لاستهداف الملايين من الناس.لفهم كيف يستخدم المهاجم الهندسة الاجتماعية

المحرر الضيف

«اليسا توريس» مدربة معتمدة في معهد SANS متخصصة في التحليل المتقدم للجرائم الالكترونية والاستجابة للحوادث والهجمات الالكترونية. لها خبرة جيدة في معالجة الحوادث وتعمل مع فريق أمن داخلي كمحققة و خبيرة فى الطب الرقمي. يمكنك متابعة أليسا على تويتر @sibertor.

دعونا نلقي نظرة على المثال التالي:

تلقيت مكالمة هاتفية من شخص يدعي أنه من شركة دعم أحد برامج الحاسب الآلي، مايكروسوفت مثلاً. يخبرك المتصل أنه لاحظ أن جهازك يعمل بشكل غريب وأنه يعتقد أن سبب ذلك هو أن جهازك مصاب بأحد البرامج الخبيثة. كما يخبرك بأنه مكلف من قبل الشركة للتحقيق في الامر ومساعدتك على حماية جهازك. وبعد ذلك يستخدم هذا المتصل مجموعة متنوعة من المصطلحات التقنية لاقناعك أن جهازك مصاب.

على سبيل المثال، قد يطلب منك أن تتحقق من وجود بعض الملفات على جهازك، ويخبرك كيف تستطيع العثور علي هذه الملفات. عندما تجد هذه الملفات فعلاً، فإن المتصل يؤكد لك أن وجود هذه الملفات هي علامة أكيدة على إصابة جهازك. حقيقة الأمر أنه اختار بعض ملفات نظام التشغيبل التي توجد فى أى جهاز.

بعد أن يقنعك بإصابة جهازك، ينصحك لشراء برمجيات «آمنه» من أحد مواقع شبكة الانترنت. طبعاً فالبرامج التي توجد على الموقع الذي يحدده لك تكون برامج مؤذية. أو قد يطلب منك أن تسمح له بالتحكم عن بعد في جهازك حتى يتمكن من إصلاحه. وإذا سمحت له بذلك، ففي الواقع سوف يقوم هو بأصابة جهازك.

ضع في الاعتبار أن الهجمات الهندسة الاجتماعية لا تقتصر فقط على المكالمات الهاتفية. أنها يمكن أن تتم من خلال أي تقنية اتصال تقريباً،

الهندسة الاجتماعية

وذلك يشمل هجمات التصيد عبر البريد الإلكتروني والرسائل النصية، ورسائل «الفيسبوك»، ومشاركات «تويتر» أو المحادثة عبر الإنترنت. والمفتاح هو أن تكون حذراً.

معرفة كيفية منع وكشف ووقف هجمات الهندسة الاجتماعية هي واحدة من الخطوات الأكثر فعالية التي يمكنك اتخاذها لحماية نفسك.

كيفية اكتشاف ووقف هجمات الهندسة الاجتماعية

أبسط طريقة للدفاع ضد هجمات الهندسة الاجتماعية هي استخدام الحس السليم. إذا كان هناك شيء يبدو مشبوها، فانه قد يكون هجوماً. بعض المؤشرات التي تدلك أنك تتعرض لهجوم الهندسة الاجتماعية ما يلي فكن حذرا فقد يكون أحد مجرمي الشبكة:

- شخص ما ألح عليك إلحاحاً شديداً ويجعلك تشعر بأنك تحت ضغط لاتخاذ قرارك بشكل سريع جداً.
- شخص يسأل عن معلومات يجب ان يكون ممثل الشركة يعرفها أو معلومات تشعر أنه ليس لها علاقة بموضوع الاتصال.
- شخص يخبرك أنك ربحت مبلغا كبيراً من المال أو أن يعرض عليك بعض البرامج الباهضة الثمن بسعر زهيد أو بدون مقابل.

إذا بدأت تشك في أن الشخص الذي يتصل بك هو أحد مجرمي الشبكة وهذا قد يجعلك ضحية لهجوم الهندسة الاجتماعية، فعليك قطع الاتصال به فوراً. إذا كان التواصل من خلال الدردشة معك على الانترنت، عليك إنهاء الدردشة. إذا كان التواصل من خلال البريد الإلكتروني فعليك حذف الرسالة. إذا كان هذا الهجوم له صلة بجهة عملك، عليك ابلاغ الادارة المختصة بأمن المعلومات لاتخاذ اللازم وتحذير بقية الموظفين.

كيف تتفادى الهجمات المستقبلية

لحسن الحظ هناك بعض الاحتياطات التي يمكنك اتخاذها للمساعدة لحماية نفسك ضد هجمات الهندسة الاجتماعية المستقبلية.

- **لا تفصح عن كلمات السر الخاصة بك لأحد:** لا توجد شركة أو شخص يقوم بالاتصال بك و يسألك عن كلمة السر الخاصة بك.

الهندسة الاجتماعية

- **لا تفرط من نشر معلومات تخصك:** كلما عرف المهاجم معلومات أكثر عنك، أصبح من الأسهل بالنسبة له إيجاد طرق لتضليلك. حتى التفاصيل الصغيرة عنك، يمكن وضعها معا لرسم صورة كاملة لك. كلما قللت المعلومات المنشورة عنك، بما في ذلك مشاركاتك على مواقع التواصل الاجتماعية و قوائم البريد الالكترونى، كلما قل احتمال مهاجمتك.

- **تحقق من جهات الاتصال:** في بعض الأحيان قد يتم الاتصال بك من قبل المصرف الذي تتعامل معه، شركة بطاقة الائتمان، مزود خدمات المحمول أو غيرها لأسباب مختلفة. إذا كان لديك أي شك حول طلب الحصول على المعلومات، اطلب من الشخص المتصل الاسم ورقم الهاتف. ثم أبحث بنفسك على رقم هاتف الشركة من مصدر موثوق، مثل الرقم على الموجود على بطاقة الائتمان الخاصة بك أوالرقم الموجود على كشف حسابك المصرفي . بهذه الطريقة عند أتصالك بالشركة تتأكد فعلاً من أنهم أتصلوا بك. على الرغم من أن هذا فيه بعض المشقة، الا أن حماية هويتك ومعلوماتك الشخصية تستحق هذه المتاعب الإضافية.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول الى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة http://www.securingthehuman.org.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة المتخصصين في أمن المعلومات بكلية علوم وهندسة الحاسب الآلي بجامعة الملك فهد للبترول والمعادن.

مصادر إضافية

عدد أوتش " هجمات تصيد المعلومات عبر البريد الإلكتروني ": http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_aa.pdf

عدد أوتش " إستخدام الشبكات الإجتماعية بأمان ": http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201303_aa.pdf

تفادي الاحتيال (باللغة الانجليزية): http://www.onguardonline.gov/topics/avoid-scams

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي
ترجمها إلى العربية: طلال موسى الخروبي، فرج أحمد عز الدين.