تجنب مفهوم الهندسة الاجتماعية وهجمات الاصطياد "Social Engineering"

لا تقدم معلومات حساسة لأي شخص ما لم تكن متأكدا من هو بالضبط وأنه يستحق الوصول إلى تلك المعلومات.

ما هي هجمات الهندسة الاجتماعية Social Engineering ؟

لشن هجمة من نوع الهندسة الاجتماعية Social Engineering يستخدم المهاجم التفاعل الإنساني (المهارات الاجتماعية) للحصول على معلومات أو المساومة على معلومات حول منظمة أو نظامها الحاسوبي. قد يبدو المهاجم محترما ومتواضعا، وقد يظهر أنه موظف جديد، فني تصليح، أو باحث وقد يظهر دلائل على ذلك الادعاء. ولكن بطرح بعض الأسئلة قد يستطيع تجميع نتف معلومات تساعده على اختراق شبكة المنظمة. إذا لم يتمكن المهاجم من جمع معلومات كافية من مصدر واحد فقد يتصل بمصدر آخر في نفس المنظمة ويعتمد على المعلومات التي استقاها من المصدر الأول ليضيف إلى مصداقيته.

ما هي هجمة الاصطياد "Phishing Attack"؟

هي شكل من أشكال الهندسة الاجتماعية Social Engineering. تستخدم هجمات الاصطياد الرسائل الالكترونية ومواقع الانترنت الخبيثة للحصول على معلومات شخصية وغالبا مالية. قد يرسل المهاجمون رسائل الكترونية من شركة بطاقات ائتمان ذات سمعة أو من مؤسسة مالية تطلب معلومات عن الحساب مدعية في الغالب وجود مشكلة. عندما يقدم المستخدمون المعلومات المطلوبة يمكن للمهاجمين استخدامها للوصول إلى الحسابات.

كيف تتجنب أن تكون ضحية لمثل هذه الهجمات؟

- كن حذرا من أي مكالمات هاتفية مشكوك فيها، أو زيارات أو رسائل الكترونية من أفراد يسألون عن موظفين أو عن معلومات داخلية أخرى. وإذا ادعى شخص مجهول أنه من منظمة قانونية حاول التحري عن هويته من الشركة مباشرة.

- لا تقدم معلومات شخصية أو معلومات عن منظمتك بما في ذلك بنيتها التنظيمية أو شبكاتها ما لم تكن متأكدا من السلطة المخولة للشخص للحصول على تلك المعلومات.
- لا تكشف معلومات شخصية أو مالية من خلال الرسائل الألكترونية ولا ترد على رسائل تطلب مثل هذه المعلومات. ومن ذلك متابعة الروابط المرسلة بالبريد الألكتروني
- لا ترسل معلومات حساسة عبر الانترنت قبل التأكد من سياسة أمن الموقع أو الحصول على دليل أن المعلومات يجري تشفيرها. من مؤشرات التشفير URL التي تبدأ بـــ :https وأيقونة padlock icon أسفل نافذة المتصفح browser
- انتبه للرابط "URL" في الموقع على الشبكة. قد تبدو المواقع مطابقة لمواقع شرعية ولكن ال URL قد يستخدم اختلافا في التهجئة أو مجالا آخر (ex..com vs..net)
- إذا لم تكن متأكدا أن طلبا بواسطة البريد الألكتروني شرعي حاول التحقق منه بالاتصال بالشركة مباشرة. لا تستخدم معلومات اتصال مقدمة على موقع على الشبكة مرتبط بذلك الطلب. وبدلا من ذلك قم بمراجعة معلومات الاتصال السابقة. المعلومات حول هجمات الاصطياد المعروفة متاحة كذلك على الشبكة من مجموعات مثل مجموعة العمل لمكافحة الاصطياد
- حمّل واحتفظ ببرنامج مضاد للفيروس وحوائط نارية ومصافي الرسائل الالكترونية للتقليص من حركة المرور هذه (لمزيد من المعلومات يرجى مراجعة الموقع http://www.antiphishing.org/phishing_archive.html)

ماذا تفعل إن شعرت أنك ضحية لهذه الهجمات ؟

- إذا شعرت أنك كشفت معلومات حساسة حول منظمتك فأخبر بذلك الأشخاص المناسبين في المنظمة بمن في ذلك مديري الشبكات. يمكن تنبيههم إلى أي نشاط مشبوه أو غير عادي
- إذا كنت تعتقد أن حساباتك المالية مهددة اتصل بمؤسستك المالية فورا وأغلق أي

- حساب يمكن أن يكون قد اصبح مكشوفا. راقب أي تكلفة على حسابك لا يمكن تفسيرها.

المؤلف : ميندي مكدويل
إنتاج جامعة كارنيجي ميلون سنة 2007. تمت إعادة إنتاجه بواسطة كيوسيرت مع أخذ الترخيص