بسم الله الرحمن الرحيم

جامعة الملك سعود
كلية علوم الحاسب و المعلومات
قسم نظم المعلومات

الهندسة الأجتماعية و كيفية الحماية منها

إعداد:
محمد الرشيدي

مقدمة:

في صباح يوم من الأيام تمكنت مجموعة من الغرباء من الدخول لمقر إحدى شركات الشحن الكبرى و الوصول إلى كامل الشبكة الداخلية لشركة والحصول على معلومات حساسة و مهمة عن تلك الشركة ، و كل هذا حدث من دون أي تصريح رسمي لهم من رئيس الشركة أو حتى مجرد إذن لهم بالدخول لمقر الشركة. فالسؤال الذي يتبادر إلى الذهن الآن كيف أستطاعوا عمل ذلك !؟.
لقد تمكنوا هؤلاء الأشخاص من الدخول إلى العديد من الأماكن عن طريق الحصول على إذن دخول لكل موقع على حده من العديد من الموظفين الذين قابلوهم في الطريق. ففي البداية وقبل كل شئ قاموا بعمل بحث بسيط عن الشركة لمدة يومين و ذلك قبل حتى مجرد وضع أقدامهم على بوابة الشركة الرئيسية. فعلى سبيل المثال، قاموا بمعرفة أسماء الموظفين الرئيسين بالشركة عن طريق الأتصال بإدارة الموارد البشرية والإدعاء بأنهم أحدى شركات الأعلانات و يحتاجون أسماء هؤلاء الموظفين، وبعد أن جمعوا كل المعلومات التي يحتاجونها قاموا بتنفيذ عملية الدخول لمقر الشركة. ففي البداية أدعوا أنهم أضاعوا مفتاح الباب الأمامي فسمح لهم الموظف بالدخول. وعند وصولهم إلى الطابق الثالث و الذي كان يعتبر منطقة محمية ببوابات إلكترونية أدعوا أيضا أنهم أضاعوا بطاقات الهوية الخاصة بالشركة و بأبتسامة وعلى نحو ودي قام الموظف بالسماح لهم بالدخول وقد أقتنع بقصتهم المزيفة. ومن نتائج البحث الذي قاموا به قبل عملية الدخول أنهم عرفوا أن الرئيس المالي للشركة كان في إجازة وقد سافر خارج البلاد ولذلك تمكنوا من الدخول أيضا إلى مكتبه الشخصي والحصول على معلومات الشركة المالية التي وجدوها بحاسبه الشخصي و الذي كان متروك غير مغلقا. بعد ذلك قاموا بالأتصال بقسم الدعم الفني وتقليد صوت الرئيس المالي (فقد قاموا بمعرفة نبرة صوته مسبقا) و طلب كلمة المرور الخاصة به للدخول للشبكة. وبعد دخولهم للشبكة قاموا بإستخدام بعض برامج الأختراق (Hacking) و تمكنوا من الوصول إلى مناطق أكثر في الشبكة.
في الحالة السابقه أدعى هؤلاء الأشخاص أنهم خبراء شبكات و قد طلب منهم الرئيس المالي من عمل تدقيق أمني له من دون علم الموظفين، مستغلين عدم وجود الرئيس، و لذلك أستطاعوا خداع كل من واجههم في الطريق من الموظفين بما في عملية الدخول لمكتب الرئيس المالي و كل تلك الحوادث تمت عن طريق مايعرف بالهندسة الأجتماعية.

تعريف الهندسة الأجتماعية:

تعرف الهندسة الأجتماعية على أنها عملية خداع الأشخاص الآخرين و ذلك للحصول على دخول غير شرعي لبيانات أو أنظمة أو حتى شبكات بأكملها ويمكن أن يكون المستهدف إما شخص أو شركة. و عادة ما يمتاز المحتالون بمهارات إجتماعية جيدة مثل الأقناع و القبول لدى الآخرين. ويعتمدون على بعض الحقائق النفسية للبشر مثل نزعة الأشخاص إلى حب المساعدة و التعاون و اللجؤ للآخرين في حل المشاكل و حب التحرر من المسؤلية في حالة حدوث مشكلة ما. كما يعتمدون على الخصال لبعض الأشخاص مثل السذاجة والبساطة والأهمال لدى الناس.

فالمحتالون يستغلون كل ماسبق لكسب ثقة المستخدمون بأفتعال أوضاع معينة. مثلا (حالة الطوارئ. اللطافة و الكلام المعسول. التهديد و إستخدام السلطة).

أهدافها:

بشكل عام تكون أهداف الأشخاص الذين يعتمدون على الهندسة الأجتماعية هي نفسها أهداف المخترقون (Hackers)، فهم يهدفون إلى الحصول على وصول غير شرعي إلى معلومات الآخرين و التي يمكن أن تكون لأشخاص عاديين أو شركات و منظمات حكومية و خاصة.
فعلى سبيل المثال يمكن للمحتال الأتصال بالضحية و الأدعاء بأنه من موظفين البنك الذي يتعامل معه الضحية و في السيناريو التالي مثال على ماقد يحدث في المحادثه.

سيناريو:

يقوم الشخص المحتال بمراقبة العميل عند قيامه بعملية فتح الحساب، و أثناء خروج العميل من البنك يأخذ المحتال رقم لوحة السيارة الخاصة بالعميل والذي يمكنه من الوصول إلى إسم العميل و رقم هاتفه.
بعد ذلك يقوم المحتال بالإتصال على الضحية خالد في الساعة الثامنة و النصف صباحا كما في المحادثة التالية:
المحتال: صباح الخير، هل يمكنني التحدث إلى السيد خالد.
خالد: نعم أنا خالد.
المحتال: صباح الخير سيد خالد، معك صالح (ويستخدم أسم مزور) موظف من فرع بنك الشموع الذي فتحت حسابك الشخصي فيه و أنا آسف لأني أتصلت عليك في وقت مبكر (ويتحدث بكل ثقة).
خالد: أوه من بنك الشموع، لقد كنت أتناول وجبة الأفطار و لكن لايهم.(الضحية قد تفاجأ بالأتصال).
المحتال: لقد قمت بأخذ بياناتك الشخصية من النموذج الذي قمت بتعبئتة عند فتحك للحساب لدينا وقمت بالأتصال بك ويؤسفني أخبارك أنه حدث لدينا عطل مفاجئ في الحاسب المركزي لدينا في مساء البارحة ونحاول الآن إسترجاع جميع بيانات عملاء البنك.

خالد: عطل!؟ و هل ضاعت جميع بياناتي.
المحتال: لا ياسيدي، سيمكننا من إسترجاع جميع بيانات العملاء ولكن نحتاج إلى بعض البيانات منك حيث لايمكننا الآن من أستخدام نظام البنك لمدة اليوم كاملا.

و يقوم المحتال من أخذ البيانات من الضحية عن طريق أخذ البيانات العامة وصولا إلى المعلومة التي يريدها حتى لا يثير الشك تجاهه وفي هذه الحاله يريد المحتال الوصول إلى بيانات البطاقات الأئتمانية للضحية.
المحتال: شكرا ياسيد خالد على تعاونك و تفهمك معنا و سنقوم من إسترجاع جميع بياناتك الآن و سيمكنك إستخدام حساباتك لدينا خلال الخمسة عشرة دقائق القادمة و نرجو أن لاتترد من الأتصال بنا في حالة وجود أي مشكلة معك.
خالد: شكر و إلى القاء.
المحتال: إلى اللقاء.

وسائلها:

تكون طرق الأختراق عن طريق الهندسة الأجتماعية على مستويين: المستوى المحسوس(أو المادي) و المستوى النفسي. ففي المستوى المحسوس يمكن إستخدام أماكن العمل،الهاتف أو مكب النفايات الورقية. ففي أماكن العمل يمكن للمحتال المشي عبر بوابة الشركة و هو متنكر بزي عامل صيانة، أو أن يزعم أنه مستشار من جهة أخرى و يجب أن يدخل إلى الشركة حيث يوجد إجتماع في الداخل و يجب عليه أن يكون متواجد هنالك.
أيضا رسالة "غير موجود في المكتب" المعتادة تشير إلى أن شخصا ما ليس في المكتب و حتى تاريخ معين وفي الغالب لن يقرأ بريده طوال فترة غيابه. وهذا قد يسهل عمليات احتيالات و تلاعب من قبل المحتالين. بالنسبة للمحتال، هذه معلومات قيمة جدا. إليك مايراه المحتال في الرسالة:

1. الشخص المعني خارج البلد. هذه المعلومة تسهل على المحتال إنتحال شخصية الشخص الغائب.
2. غالبا فإن الشخص الغائب لن يقرأ بريده الألكتروني و بذلك لن يكون هنالك طريقة لإكتشاف المحتال حتى عودته.
3. يمكن استغلال غياب الشخص المعني، و الإتصال بزميله أو الشخص البديل عنه لطلب معلومات حساسة أو مساعدة ما. فمثلا: لو كان أحمد بديل لسعد فإن المحتال يتصل على أحمد "الأخ أحمد، سبق و أن أتفقت مع الأخ سعد على إعطائي معلومات بخصوص المشروع و لكنه الآن غير موجود. فهل من الممكن أن أعتمد عليك في ذلك".

و حتى في مكب النفايات يمكن للمحتال الحصول على معلومات تساعده كثير مثل دليل هواتف الموظفين و أسماءهم ،التقارير المالية للشركة، سياسات الشركة، مذكرات الإجتماعات، الأقراص الصلبة لأجهزة الحواسيب حيث يمكنه إسترجاع البيانات المحذوفها منها عن طريق بعض البرامج.....إلخ.
أما على المستوى النفسي، فالمحتالون يبنون بعض حيلهم على بعض الحقائق النفسية، فهم بذلك يستطيعون وضع الضحية في وضع نفسي مناسب حتى يستطيعون الوصول إلى هدفهم عن طريق كسب الثقة أو الكلام المعسول أو أن يدعي أنه شخص ما مثل ما حدث في السيناريو السابق. وبغض النظر عن الطريقة التي يستخدمونها يبقى هدفهم الجوهري هو أن يقنعون الشخص بالكشف عن البيانات التي لديه.

طرق الحماية منها:

- قبل الإدلاء بأي معلومات، تأكد من أن الشخص الذي يطلب المعلومات هو حقا من يدعي. وإذا كان يسأل عن معلومات حساسة أو الدخول إلى الشركة شخصيا أو إلكترونيا، ربما من الأفضل أن تتأكد من صحة أقواله عن طريق الشركة التي يدعي الأنتماء إليها، أو التشاور مع المدير في شركتك إذا لم تستطع التأكد من هويته عن طريق دليل الشركة.
- إذا أراد أحدهم محادثتك بشأن فرص العمل، حافظ على موضوع الحوار حول مهاراتك و ليس حول مشاريعك التي تعمل فيها.
- أحذر من البريد الإلكتروني الذي يحمل معه مرفقات و لاتفتح مرفقات رسائل البريد الإلكتروني إلا إذا كنت تثق بمرسلها. المرفقات ممكن أن تحتوي فيروس أو طروادة. فإذا أستلمت الرسالة في البريد الإلكتروني من شخص تعرفه لكن عنوان الملف المرفق أو الرسالة نفسها غريب نوعا ما، فمن الممكن أن تحتوي الرسالة على شيفرة ضارة. إفحص المرفقات ببرنامج مضاد للفيروسات قبل فتحها.
- إذا رأيت شخصا غريبا في منشآت الشركة، اسأل ما إذا كان هذا الشخص موظفا. إن لم يكن كذلك أعرض عليه المساعدة بمرافقته إلى الردهة أو أي مساعدة أخرى.
- لاتكتب كلمة السر حيث يسهل إيجادها.
- كن حذرا عندما تتكلم في الأماكن العامة، فالناس يصغون لك، فلا تناقش المواضيع السرية.
- لا تثق إلا بمن تعرفه إذا كان الموضوع يخص تحويل مبالغ إلى حساب خاص لك بالبنك وكن حريصا جدا في تداول بطاقتك الائتمانية ولا تفصح عن أرقامك السرية الخاصة بالبنك لأي أحد مهما كان وكن حريصا عند إدخالها أن لا يراها أي أحد.

خاتمة:

تعتبر عملية إستخدام الهندسة الإجتماعية من الوسائل التي لا تتطلب أي معرفة مسبقة أو عميقة بتقنيات الحاسب بشتى أنواعها، فهي تعتمد على بعض الحقائق النفسية و الإجتماعية للبشر. كما أنها تعتبر من الأخطار التي لايمكن حسابها بطريقة مباشرة أو التنبؤ بها و لايوجد أنظمة متكاملة لمنع حدوث عملية التحايل. فكثير من الشركات تركز كامل إهتمامها على وسائل الأمن الأخرى مثل عملية حماية الشبكة الداخلية للمنشأة بإستخدام الجدر النارية أو أنظمة كشف التسلل، ولكنهم يغفلون الجانب الأمني للهندسة الإجتماعية. فمهما حصنت الشركة مواردها بأحدث و أقوى أنظمة الحماية الحاسوبية يمكن إختراقها بالإستخدام الجيد للهندسة الإجتماعية. فلذلك يجب على الشركة الأخذ بعين الإعتبار لمخاطر الهندسة الإجتماعية أثناء وضعها للسياسات و الإجراءت الأمنية الخاصة بها، كما ينبغي التوعية و التدريب للموظفين فهم يعتبرون الوسيلة الأساسية للهندسة الإجتماعية.

المراجع:

[1] D. Gragg, "A Multi-Level Defense Against Social Engineering", SANS Institute, 2003.
[2] R. Gulati, "The Threat of Social Engineering and Your Defense Against It", SANS Institute, 2003.
[3] M. Ciampa, "Security+ Guide to Network Security Fundamentals", 2nd edition, Thomson, 2005.
[4] S. Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics", http://www.securityfocus.com/cgi-bin/infocus.pl?id=1527, Dec. 2001
[5] S. Granger, "Social Engineering Fundamentals, Part II: Combat Strategies", http://online.securityfocus.com/infocus/1533, Jan. 2002.
[6] S. Brenner, "The Psychology of Social Engineering", http://cybercrimes.net/Property/Hacking/Social%20Engineering/PsychSocEng/PsySocEng.html, Jul. 97.
[7] J. RUSCH, "The Social Engineering of Internet Fraud", http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm.
[8] "Protecting the Company's Information", Part of Corporate Security Awareness Program by Symantec Corporation.