بسم ا الرحمن الرحيم

كلنا سمعنا عن كيفن متنيك الأسطورة ولكن للأسف كانت المعلومات التي تعطيها لي المواقع العربية كلها لا تتعدى صفحة أو اثنين وكلها متشابهة لذا وبعد أن اطلعت عليه وأجريت الكثير من الأبحاث حوله في المواقع العالمية
وبعد قراءتي لكتبه التي ألفها بنفسه والتي الفت ضده وكل المقالات التي تحدثت عنه قررت ووجدت فيها من المعلومات ما لا يستغني عنها أي هاكر أو مختص في الأمن التقني لذا ابدأ بكتابه الأول وهو

THE ART OF DECEPTION

مع ملاحظة انه قد تم حذف بعض المواضيع الغير هامة والمملة للقارئ وبعض التفاصيل السخيفة
على أن أترجم لكم باقي الكتب ولنا سلسة ستنشر لاحقا وهي مجموعة من الكتب المهمة التي لم يتم ترجمتها من قبل
طبعا سيتم نشر الكتب واحد تلو الآخر

كل سبت ابتداء من 24/12/005 سيتم نشر فصل من الكتاب إلى أن ينتهي وسينشر الكتاب كاملا في الأسبوع الأخير

يمكنكم ترشيح الكتاب الذي ترغبون بترجمته أو أي استفسار أخر يمكنكمالتراسل من خلال
Freedontelloo@gmail.com

ترجمة : فريدون تيللو قراءة وتدقيق : سردار سليمان

سوريا – القامشلي-رميلان

لا تنسونا من دعوة صالحة

المقدّمة:

يُحطِّم بَعْض الهاكرز ملفاتَ الناسَأَو كامل الأقراص الصلبةِ؛ هؤلاء يَدْعونَ الهاكرز إي اللصوصَأو مخربون. بَعْض الهاكرز المبتدئون لا يُكلفون أنفسهم عناء تَعَلّم التقنيةِ، لكن ببساطة عن طريق البرامج وأدوات هاكر آخر لـ تحميلِو لاقتحام أنظمةِ الحاسوب؛ هم يَدْعونَأطفال التصفح. الهاكرز أكثر خبرة بالبرمجة العليا وِ يُطوّر الهاكرز البرامج وتُعيِّنهم لاختراق الويبِو الأنظمة . وبعد ذلك هناك الأفرادَ الذين لَيْسَلهُمْاهتمام في التقنيةِ، لكن يَستعملونَ الحاسوبَكمجرّد أداة لمُسَاعَدَتهم في سَرِقَة المالِ،سلع، أَو خدمات. وبالرغمالتشويه من قبل أجهزةَ الإعلام يقول كيفن متنيك لَستُ لصّكومبيوتر خبيث. لكنني طورت نفسي.

البَداية:
مسيرتي كانت على نحو مبكر. كطفل سعيد، لكن سريع الملل .بَعْدَ غياب والدي وانأ في الثالثة،عَملتْأمي كنادلة لتعيلنا .فكانت الإنسانة التي كرست حياتها لتراني اكبر يوم بعد يوم رغم كل الصعاب التي تعرضنا لها البداية كانتفي مدينة سان فرنان دو فالي منحني المجال لاستكشاف معالم لوس أنجلس ، وبعُمرِ أثنا عشرَاكتشفت طريقة لركوب الحافلات مجانا في كافة أنحاء لوس أنجلس ِ من خلال بعض الأسئلة التي كانت تبدو بريئة من قبل طفل صغير واستطعت إن أتحايل على جهاز قطع التذاكر . (منذ الصغر تمتعتبذاكرة كانت ولا تزال تمكنني من تَذكُّر أرقامَ الهواتف، كلمات سر، والتفاصيل التافهة الأخرى.) الهواية الأخرى التي ظهرت في عُمرِ مبكّرلدي كَانَت ولعي بالتقنية فما إن أرى جهازا أو برنامج حتى أبدا تعلمه واتقانة وتطويره هذه كانت المتعةَ في كَسْب إسرار المعرفة.

التحول مِنْ لص الهاتف إلى لصِّ الكومبيوتر:

لقائي الأول مَع ما تعلّمت تسميته في النهايةَ الهندسة الاجتماعية.

؟؟الهندسة الاجتماعية هي التي نسميها نحن خداع الناس أو النصبأي أن تتحايل على شخص لتأخذ منه معلومات تحتاجها لعمل معين وقد اختار لها كيفن هذا الاسم لذا سوف نستخدمه في ترجمتنا للكتاب؟؟

حَدثتْأثناء سَنَواتِلدراسة في المدرسة العليا عندما قابلتُطالباً آخراً منغمسَفي هواية التحايل على المقاسم الهاتفية. وهو نوع أخر من الهاكر الذي يدخل شبكةِ

الهاتفَباستغلال أنظمةِ الهاتفَأو الزبائن أنفسهم . أطلعني صديقي على خُدَعَ لطيفةَ مع الهاتف، مثل الحُصُول على أيّ معلومات عن زبون معين لدى إحدى شركات الهاتفَ ،واستعمال اكواد سرية خاصة بالشركةِلإجراء مكالمات خارجية مجانيةِ. (في الحقيقة كان مجانا بالنسبة لنا فقط. اكتشفت كثيراً فيما بعدً بأنّ الاكواد لا تمكننا من إجراء مكالمة مجانية وإنما تضاف المكالمة على حساب شخص آخر
تلك كَانتْ بداياتي. صديقي و صديقه الذي كان ملك قرصنة الهواتف اسمعاني النداءاتَ الزائفة إلى شركةِ الهاتفَ على نحو خدع موظفو الشركة؛ تَعلَّمت خداع مختلف شركات الهاتفِ، تدربت طويلا على خداع الآخرين وانتحال الشخصية ْ.
حتى تفوقت على من علموني ذلك. الدرس الذي اثر على مجرى حياتي لخمسة عشر سنة التالية.
، إحدى مزحِاتي المفضّلة كَانت اختراق مقسم هاتف المدرسة والدخول إلى حساب صديقي ملك قرصنة الهواتف.
فعندما حاول الاتصال مِنْ البيتِ، سمع رسالة تُخبرُه بان رصيده غير كاف لإجراء أي مكالمة أصبحت خبير اتصالات، لَيسَ فقط الإلكترونياتَ، المقاسم،
والكومبيوترات، لكن أيضاً كل ما يتعلق بالشركاتَ، والإجراءات التي يتبعونها ، أكثر من أي خبير اتصالات آخر . بعمر سبعة عشرَ سنةً، كُنْتُ قادرا على مُنَاقَشَة أكثر موظفي Telco عن إي قسم و موضوع مَعهم شخصياً أَو بالهاتفِ بَدأتْ رحلتي المشهورة جداً في المدرسة العليا لا أَستطيعُ وَصْف التفاصيلِ هنا، يكفي القول إن ما دفعني بكل قوة في هذا المجال إن اقبل في شلة الهاكر. استعملنا تعبير الهاكر لتعني الشخص الذي يقضي الكثير مِنْ الوقت يستخدم الأجهزةِ والبرامج، أمّا لتَطوير البرامج أَو لتَجَاوُز الخطواتِ الغير ضروريةِ وانجازُ العمل بسرعة أكبر. أصبحَ التعبيرُ الآن ذو صدى سيء، "مجرم خبيث." بَعْدَ تخرجي من المدرسة العليا دَرستُ الحاسباتَ مركز التقنيات في لوس أنجلس خلال بِضْعَة شهورِ، أدركَ مدير المدرسةَ باني اكتشفت ضعفاً في نظامِ التشغيل والسيطرة الكاملة كأي إداري على شركة IBM. أفضل خبراء الحاسوب لم يَستطيعوا فْهمَ كيف قمت بذلك. فقاموا باستغلالي وعرض علي ما ليس بقدرتي رفضه : العمَلُ لتَحسين أمنِ كومبيوتر المدرسةَ أو سيتم ملاحقتي قانونيا. بالطبع، اخترت أَنْ أتعاون معهم، وتخرجت بدرجة الشرفِ.

نحو المهندس الاجتماعي:

معظم الناس يعانون من الروتين في العملِ لحد الإعياء. كُنْتُ محظوظُ بما فيه الكفاية للتَمَتُّع بعملِي. ،
لا يمكن ُ تَخَيُّل التحدي، والسرور الذي تملكني كمحقّق خاصّ. كُنْتُ أطور مواهبَي في فنِ الأداء ما اسميه هندسة اجتماعية (تدفع الناس للقيام بأمور لصالحك وبالتالي هم من يدفع الثمن في النهاية).

بالنسبة لي لم تكن هناك صعوبة في الهندسة الاجتماعية. فعائلة أبية كَانَت في التسويق لأجيالٍ، لذا فَنّ التأثير والإقناع كَان ميزةً مَوْرُوثةً. عندما تَجْمعُ تلك الميزةِ بميلِ لخَدْع الناسِ عندها تملك لمحةُ عن حياة المهندس الاجتماعي المثالي.

عَملتُ على تَطوير مهاراتِ حرفتِي، أَدْعوها حرفة،
كَأ نَ أَنْ يَختارَ موضوع غير مهمة لي وأَرى إذا كنت استطيعُ أَنْ أناقش شخص ما على ا لهاتفِ في ذلك الموضوع وأبدو له إني اعرف جيدا عما أتحدث ، فقط لتَحَسّينْ مهاراتَي. بالطّريقة نفسها كُنْتُ أُزاولُ خُدَعَي السحريةَ، زاولتُ التَحَجُّج. خلال هذه التدريباتِ، وَجدتُ قريباً بأنّني يُمْكِنُ أَنْ احصل على أيّ معلومات أريدها.

كما وَصفني ليبرمان وطومسون في شهادتهما أمام الكونغرس

؟؟ليبرمان وطومسون هما عضوان في الكونغرس الأمريكي وهما اللذان ناقشا قضية كيفن في الكونغرس بعد إلقاء القبض عليه؟؟

بعد فترة تمكنت من اختراق أنظمةِ الحاسوب في بعض مِنْ اكبرِ الشركات على الكوكبِ، واختراق لبعض مِنْ أنظمة الحاسوب المختصة بالبرمجيات الأمنية المتطورة جداً. استعملت في ذلك وسائل مختلفة تقنية وغير تقنية للحُصُول على النسخ الأصلية لأنظمةِ التشغيل المُخْتَلِفةِ لدِراسَة نقاطِ ضعفهم وطرق عملها. كُلّ هذا كان كفيلاً بإرضاء فضولَي لاكتشاف قدراتي

الخلاصة:

اعترفت منذ إلقاء القبض علي بأنّ أعمالي كَانتْ غير شرعيه ولكن كل ما فعلته كان بدافع الفضول أردتُ أن اكتشف مهاراتي. تحولت بعد ذلك من الطفل المشاكس إلى ذلك الهاكرز الأكثر شراسة في العالم وأصبحت كابوسا تخَافَه الشركاتِ والحكومةِ. كان كل ذلك انعكاس لل 30 سنة القاسية التي مضت من عمري الآن لم اعد كما كنت عليه في سابق عهدي لقد أصبحت شخصا آخر أوظف مواهبَي ومعرفتي لزيادة أمنِ المعلوماتِ ومساعدة الحكومة والشركات ودرع أي تهديد لأمن المعلومات لديهم.

؟؟ لقد أصبح كيفن بعد خروجه من المعتقل خبير امن ومستشار حماية وهو يدعي انه ترك الاختراق وهذا موضوع يكثر الجدل فيه؟؟

الفصل الأول

إيجاد الثغرة الأضعف

لا تدخر الشركات جهدا أو مالا في سبيل زيادة أمنها سواء بشراء أفضل ما توصل له الأمن التقني و رفع كفاءة موظفيها و الحراسة المكثفة لمباني المؤسسة.

مع ذلك تبقى الشركة ضعيفة بما فيه الكفاية

أما الأشخاص فإنهم يتبعون كافة الإرشادات الأمنية الموصى من ذوي الخبرة و استخدام برامج الحماية

مع ذلك يبقون ضعفاء بما فيه الكفاية.

.

العَامِل البَشَرِيّ

في شهادتي أَمام الكونغرس، وضُّحت بأنه يُمْكِنيُ الحصول على كافة المعلومات الحساسة و كلمات السر وذلك بانتحال شخصية شخص آخر مثلا مسؤول كبير في الشركة .

من المسلم به أننا تواقون للإحساس بالأمان الكامل. مما يؤدي إلى الشعور الزائف بالأمن وانه ما من مخاطر محدقة..

لا يوجد أمان كامل مهما استخدمت من وسائل و إجراءات لِماذا؟

لأن العَامِل البَشَرِيَّ هو النقطة الأضعفِ.

الأمن أيضاً في أغلب الأحيان مجرّد وهمُ، له نتائج كارثية أحيانا عند التصرف بغباء . هناك قول مأثور عن. العالم الـ مِنْ خبراء تقديرا ، ألبرت آينشتاين، ،"فقط شيئان لانهاية لهما، الكون والغباء الإنساني، " في النهاية، هجمات الهندسة اجتماعية توتي ثمارها أمام الأغبياء المتجاهلون للقواعد الأمنية.، العديد مِنْ خبراء تكنولوجيا المعلوماتِ

يقعون فريسة فكرة إنهم جَعلوا الشركات محصّنة بشكل كبير ضدّ الهجوم اعتمادا علىً مُنتَجات - برامج حماية، أنظمة تعقّب المتطفلين، أَو أدوات تحقُّق أَقوى مثل رموزِ أساسها الوقتَ لاعتقاد السائد إن المنتجات الأمنية فقط توفر الحماية الكافية.هذا كله مجرد وهم . فهذا اعتقاد موجود فقط في الخيال سيندم عليه أصحابه.ولقد أشار مستشار أمني بارزِ وهو بروس شناير إن الأمن ليس مجرد برامج حماية، بل ممارسة ." علاوة على ذلك، الأمن لَيسَ مشكلة تقنيةِ- بل قضية

إدارة و أشخاص. فبينما يطور خبراء الأمن بشكل مستمر أفضل تقنياتَ الأمنِ لجعل نقاط الضعف الأمني صعبة الاستغلال فبالمقابلِ،المهاجمون يعتمدون أكثر وأكثر على استغلال العنصرِ الإنسانيِ لان التغلب على العامل ا لإنسانيُ في أغلب الأحيان سهل، خالي من المخاطر.

إحدى حالات المكر التقليدية

ما هو الخطر الأكبر على ممتلكاتك ؟ ذلك سهلُ:
المهندس الاجتماعي -- ساحر عديم الضمير لا يمكنك إدراك ما يفعل و هو معك . ودودا جداً في أغلب الأحيان ومرح،
يدفعك للامتنان له بَعْدَ أَنْ صادفتَه.

انظر إلى هذا المثال عنِ الهندسة الاجتماعية:
لازال البعض يذكّرُون الشابَّ ستانلي مارك ريفكن ومغامرته الصَغيرة بإحدى مصارف لوس أنجلس. تفاوتتِ الأقاويل عنهُ، وهو (مثلي) لم يسبق أن نشر قصته من جهة نظره الخاصة، لذا فيما يلي مستند على التقاريرِ المَنْشُورةِ.

اختراق الكود:
في 1978, مَشى بتثاقل نحو قسم الحوالات في .بنك الباسيفيك ، حيث الموظّفون فقط مسموح لهم بالدخول لحساسية القسم. يتم يوميا تحويل مليارات الدولارات . وهو كان يَعْملُ لدى الشركة بِموجب عقد لتُطوُّير النظام الاحتياطي لبيانات قسم الحوالات في حالة تعطل حاسوبهم الأساسي . ذلك العمل خوله الاطلاع على إجراءاتِ وسير العمل ، بضمن ذلكموظفو الحوالات يقومون بوضع كلمات المرور المتغيرة يوميا أمامهم في مكان يسهل رويته . في احد أيام نوفمبر/تشرين الثّاني ولسبب معين ووجيه قام ستانلي بزيارة القسم.وألقى نظرة خاطفة نحو القصاصات الورقية المدون عليها كلمات المرور أي الباسوردات .، متظاهرا بأنه يدون ملاحظات حول سير إجراءات سير العمل و التأكد من حسن سير العمل .

. في هذه الأثناء، بدون أن يلاحظه احد حفظ الباسورد.ثم بعد دقائق قليلة خَرجَ

الحساب المصرفي السويسريِ

. . .
تَرْك الغرفةِ في حوالي السّاعة الثّالثة بعد الظهر،توجه نحو هاتف عمومي قرب البنك .واتصل مع قسم الحوالات .
. ليتصل مرة أخرى منتحلا شخصية ، مستشار البنك هانسن، عضو القسم الدولي.

وطبقا للمصادر فقد جرت المحادثة كالأتي:
بما انه مطلع على نحو كافي استطاع أن يقنع الموظفة التي اتصل بها ليتم بعد ذلك عملية تحويل 8 مليون دولار لحساب حدده مسبقا.هذه العملية كانت الأكبر في سرقة البنوك حيث لم يستعمل فيها السلاح وحتى الكومبيوتر. بل الخداع والمهارة الدقيقة لجمع المعلومات المطلوبة بدون إثارة الشبهات.

هذا ما يتحدث الكتاب عنه .أساليب الهندسة الاجتماعية الماكرة . وكيفية تفادي مخاطرهم
.

طبيعة الخطر:

توضح حادثة ستانلي بشكل جلي - إلى أي مدى يمكن إقناعنا على نحو خطير ومكلف جدا. هذا يَحْدثُ كُلّيوم. أنت قَدْ تَفْقدُ مالَالآن، أَو شخص ما قَدْ يَسْرقُ منه خططَمنتج جديدِ، وأنت لا تَعْرفُه حتى.القضية الجوهرية ليست انه إذا لم تتعرض لهكذا حوادث يعني انك بمنأى .بل متى ستتعرض لعملية كتلك.

القلق مُتزايد فقد أشار معهد امن الحواسيب . في استطلاع أجرته. انه في عام 2001 .إن 85 بالمائة مِنْالمؤسسات تعرضت لعمليات اختراق. نسبة عالية جدا تبين مدى تنامي الاختراق . مع العلم أن النسبة المذكورة فقط المكتشفة طبعا . من خلال خبرتي أرى إن تلك الأرقام المتناقلة عبر وسائل الإعلام مبالغ بها.لكن هذا لا يعني بعدم وجود خسائر مكلفة.

إن الفشل في وضع خطة أمنية يعني الدمار الأكيد.إن التقنيات الأمنية تفيد في ردع الاختراقات الغبية من قبل مبتدئون يدعون إنهم هاكرز.الخطر الأكبر يأتي من قبل هؤلاء المحترفون امرة.قون بهذا المجال.حيث يُركِّز هؤلاء الناسِعلى هدف واحد كلّمرة. وليس مثل الهواة، يُحاولونُاختراقكل الأنظمة. الهاوي يَختارُ الكميةَ ببساطة، يَستهدفُالمحترفين معلوماتَعالية النوعية والقيمة. إن التقنياتُمثل أدواتَ تحقُّقِ(لإثْبات الهويةِ)، مراقبة الدخول(لإدارة الدخول لملفات و مصادر النظام)، وتعقّب المتطفلين على الأنظمة (المكافئ الإلكتروني لأجراسِإنذار اللِصوصِ) ضرورية للشركات فهي تنفق على الكماليات مثل القهوة أكثر من توزيع الإجراءات المضادة الرادعة لحمايةالشركة ضد هجمات الهاكرز. العقل الإجرامي لا يَستطيعُ مُقَاوَمَة الإغراءِ، عقل الهاكرز يقوده نحو إيجاد حلول ومنافذ تعينه على تقنيات الحماية الأمنية. وفي العديد مِنْ الحالاتِ يقومون باستهداف الناسِالذي يَستعملون تلكُ التقنيات.
....

.

الممارسات الخادعة

هناك مقولة شائعة.الحاسوب الأمن هو المطفئ قول ذكي لكن خاطئَ بنفس الوقت فالواقع نقيض ذلك تماما.لان الحاسوب المطفئ يمكن تشغيله. فالخصم الذي يريد معلوماتك يمكنه الحصول عليها.بطرق و أساليب متنوعة .إنها قضية وقت و صبر و إصرار لا أكثر. وهذا ما يتحدث عنه كتاب. فن الخداع.

لهَزيمة التدابير الأمنية، فالمهاجم، أو الدخيل، أَو المهندس الاجتماعي عليه إيجاد وسيلة لتضليل المستخدم الضحية.لإفشاء المعومات. -خدعة الأثر الجاهل - لاختراقه. وذلك بخداع الموظفي و المستخدمون و التأثير.و القيام باستغلالهم لكشف المعلومات الحساسة و الإجراءات والأساليب المضادة .المهاجم.جوة أمنية يتسلل منها .المهاجم . ليس من تقنية تحمي البزنس بشكل نهائي . مثل محللي الشيفرات عند تحليل رسالة مشفرة .يبحث عن نقاط الضعف.تجاوزْ تقنيةَ التشفير. يَستعملُ المهندسون الاجتماعيون أساليب ماكرة لتجاوز التقنيات الأمنية.

سوء استخدام الثقة

في اغلب الأحيان المخترقون يتمتعون بمهارات ومواهب متعددة وشخصيات قوية فهم ساحرون ومؤدبون يسهل محبتهم ويمتازون بسرعة خلق جو من الثقة والوئام فالهاكرز محنك قادر على الحصول على معلومات مختلفة باستخدام استراتيجيات وتكتيكات مطورة. إن تقنيات امن المعلومات تقلل على نحو كبير الأخطار الناجمة من استعمال الحواسيب المعرضة للاختراق وعلى الرغم من ذلك تهمل نقطة الضعف الأكبر وهي العامل البشري على الرغم من رأينا إننا نحن البشر نبقى التهديد الأكثر خطورة على امن الآخرين

سماتنا العامة (كبشر)

فنحن في العالم الغربي وبخاصة الولايات المتحدة لسنا متنبهين للمخاطر والتهديدات فنحن لم نتعلم الارتياب يبعضنا البعض فلقد تربينا على محبة الجيران والثقة يبعضنا لنأخذ بعين الاعتبار كم من الصعب على الجيران مشاهدة شركات التأمين وهي تستولي على منازل وممتلكات الناس فهذه نقطة ضعف واضحة بالنسبة للمجتمع لكن الكثيرين يتجاهلون هذه النقطة ويعيشون في عالم وردي حتى تصيبهم الكارثة فنحن نعرف بأنه ليس كل البشر لطفاء وشرفاء لكننا نعيش وكأنهم كذلك هذه البراءة الرائعة كانت من نسيج الحياة الأمريكية ومن المؤلم التخلي عن ذلك . أمريكا أفضل الأماكن للعيش حيث الحرية رغم إنها أكثر الأماكن استعمالا للأقفال والمفاتيح معظم الناس على فرضية إنهم لن يتعرضوا للخداع من الآخرين اعتمادا على إن نسبة وجود الخداع منخفضة جدا والهاكرز يعرفون بهذا الاعتقاد الخاطئ لدا الناس

فهم يطلبون المعلومات بشكل معقول لا يثير الريبة وطوال الوقت يستغلون ثقة الضحية

البراءة المنظمة

هذه البراءة هي جزء من شخصيتنا الوطنية ظهرت بشكل جلي وواضح في أول مشروع لشبكات الحاسوب وإدارتها والتي كانت أربا نت Arpanet (شبكة وكالة مشاريع البحوث المتطورة لوزارة الدفاع) والتي كانت هي الانترنت
صممت كطريقة لتشارك في الأبحاث والمعلوممنها.لحكومة ومؤسسات الابحاث والثقافة والهدف منها كان حرية المعلومات بالإضافة إلى التقدم العلمي .كان كل ذلك بدون حماية أو بالحد الأدنى منها .لكن بظهور التجارة الالكترونية مخاطر ضعف الأمن في عالمنا المترابط تغيرت بشكل مثير ان انتشار المزيد من التقنية لا يعني إيجاد حل نهائي لمشكلة العامل البشري. إن نظرة صغيرة إلى مطاراتنا نكتشف إن الأمن أصبح أساسيا رغم قلقنا من التقاريرالإعلامية التي تشير إلى المسافرين القادرين على مراوغة الأمن والمرورمن نقاط التفتيش محملين بالأسلحة.رغم أن مطاراتنا على درجة عالية من التأهب في هذه الأوقات. هل كاشفات المعادن فاشلة؟
المشكلة ليست بالآلات المشكلة بالعاملالبشري والناس الذين يديرون تلك الآلات. موظفو الأمن يعلمون كيف يشاهدون الناس عبر الشاشات أكثر من إمكانية تقديم المساعدة إننا نجد نفس المشكلة ضمن الحكومة والشركات والمؤسسات المختلفة في كافة إنحاء العالم على الرغم من جهود رجال الأمن المحترفين فالمعلومات تبقى ضعيفة كهدف محتمل من قبل المهاجمين. الآن وأكثر من أي وقت مضى علينا إيقاف الأمنيات وان نكون أكثر إدراكا من قبل باللذين يحاولون اختراق أو مهاجمة الأسرار وأنظمة الحواسيب والشبكاتفنحن علينا الرضوخ لحاجاتنا الأمنية الوقائية فهذه المخاطر لا تبدو واقعية حتى تقع الطامة والكارثةالكبرى . لتفادي مثل هكذا عمل كارثي محتمل نحتاج إلى التعلم دائما والحذر بشدة ووقاية أصول معلوماتنا وأمورنا الشخصية والبني التحتية لذلك علينا أن نطبق الإجراءات الوقائية اليوم.

الإرهاب والخداع

المراوغة والخداع ليست حكراً على الهاكرز حيث أدركنا بشكل لم يسبق له مثيل إن العالم مكان خطير بعد الهجمات على نيويورك وواشنطن التي خلفت الكثير من الحزن والخوف في قلوبنا
الحقيقة تنذرنا بان هناك العديد من الإرهابيين الخطيرين في هذا العالم اللذين يريدون مهاجمتنا مرة أخرى لذا نحتاج إلى فهم كيفية اندماج الإرهابيين بالمجتمعات التي يريدون مهاجمتها ويلعبون أدوارا كطلاب أو جيران ويذوبون في الحشود ويخفون نواياهم الحقيقية هذه الأساليب المخادعة ستقرأ عنها في هذا الكتاب فعلى

حد علمي لم يستعمل الإرهابيون أساليب الهندسة الاجتماعية ومعامل معالجة المياه والمؤسسات الزراعية والكهرباء ومكونات البني التحتية.

؟؟يظهر كيفن هنا الشعب الأمريكي وذلك في محاولة منه للتقرب من قلوب الناس لا غرابة فهذا اختصاصه) وذلك بعد ما كتب عنه (ونحن نقلناها لكم كما هي بغض النظر عن رأينا) ؟؟ـ

حول هذا الكتاب

إن الأمن المتعلق بالشركات سؤال حساس جدا فمجرد ثغرة أمنية صغيرة قد تحدث الكارثة لكن الإفراط الأمني أيضا يقف عقبة أمام ديناميكية العمل حيث يمنع نمو وازدهار الشركة انه تحدي و من واجبنا التوصل إلى موازنة بين الأمن والتقدم

فصل 2

فَنّ المهاجم

لا حساسية المعلومات ظاهريا:

الاعتقاد الدارج إن التهديد الحقيقي يأتي من قبل الهندسة الاجتماعية.؟فما هي الخطوات الاحترازية؟إذا كان الهدف الاستحواذ على المعلومات المطلوبة بشدة.ماذا لو تم استهداف بعض المعلومات عالية الأهمية ما يعتمد عليه موظفو الشركة في أعمالهم.ما الحل؟ تشديد الحراسة حول مباني الشركة؟ الواقع غير ذلك تماما.الاختراق يبدأ بحصول الهاكر على مجرد معلومة و لو صغيرة أو بعض الوثائق التي تبدو للعيان بريئة .و غير مهمة وهي ملاحظة يوميا .لذلك لن يعار أي أهمية لحمايتها أو تقييد الوصول لها.لكن في الواقع اختراق أمن أي شركة ظاهريا لا في أغلب الأحيان من إهمال معلومات الغير قيمة ظاهريا. مُعظم المعلوماتِ الغير مؤذيةِ ظاهريا لا تقدر بثمن من قبل المهندس الاجتماعي.لمللها من دور حيوي في تنكره.هذا ما سأوضحه في هذه الصفحات. كيف يتم الهجوم أمامك وأنت ليس لديك أدنى فكرة عما يحدث.لوقت طويل، كان النظام المصرفي البريطاني صارما متصلبا.لا يمكنك فتح حساب جاري إلا بكتاب توصية من احد زبائن المصرف.مما قلل عمليات النصب. ولكن مدفوع الثمن . الأمور تغيرت وقواعد العمل تطورت و حدثت. بوجود شركات خاصة تقدم المعلومات عن أي زبون للتأكد من نظافة سجله العدلي. للأسف هو نفسها عرضة للخطر.بسؤال احد المهندسين موظفة في بنك ومع تصاعد وتيرة الاسئلة ترددت الموظفة .ومع إدراك المهندس الاجتماعي ذلك قال انه بصدد تأليف كتاب وهو بحاجة للمساعدة. ومرة أخرى انه يجري استطلاع عن ساعات العمل و الإنتاج.كانت الموظفة سعيدة بذلك مؤلف يطلب يد العون منها لكتابه. المهندس يطلب المساعدة من الضحية انه أمر من الصعب رفضه. . فأنت مهم وذو فائدة.و هذا قد يجعلك تترفع في سلم العمل.

أحرا ق السببَ المهاجم يقوم في حال كانت إحدى المصادر طريقا لإدراك الضحية بهجوم محتمل.لأنه سيعلم زملائه أو الإدارة.لذا سيكون من الخطورة تكرار المحاولة فيما بعد. عليك بإزالة الإحساس بالخطر من شعور الضحية. الأسئلة الكثيرة المريبة تزيد من حالة التأهب وهذا ينذر بالفشل الأكيد.بطلبك المساعدة مثل الادعاء بإجراء استطلاع ومن خلال أسئلة تافهة و شخصية لخلق جو من الود و الألفة إدراج سؤال مهم و لا يغيب عن بالك ملاحظة تغير نبرة صوت الضحية أم لا .بالطبع ليس كل الموظفين يقعون بسهولة عليك تعلم ومعرفة ردود أفعال الضحية و دراسة وجوههم وسلوكهم. من الغباء الشديد إنهاء المحادثة حالما تصل لمبتغاك. بضع أسئلة قليل من الحديث الأسئلة المطلوب الإجابة عنها يجب أن تكون ضمن كلام عام شخصي.لكي لا تتذكر فالأغلب ستتذكر ما جرى الحديث عنه في النهاية.

تَحليل الخدعة:

هذه بأكملها مستندة إلى إحدى التكتيكات الأساسية للمهندس الاجتماعي.الحصول على اكبر قدر من المعلومات التي هي بنظر الموظفين تافهة.

بحصولك على هذه المعلومات وعند تحدثك إلى الضحية وإدارتك مجرى الكلام ستبدو لها انك شخص مطلع وهذا يزيل التوتر والريبة.
مما يفيدك لاحقا بالتنكر بصفة احد مسؤولي الموظف الضحية .
رسالة متنبك:
من الحكمة التعامل مع كافة المعلومات بنفس القدر من الأهمية . ليس من معلومة تافهة. كما لو كانت اكواد الصراف الآلي.فما يبدو من الداخل و بنظر الموظفين عديم القيمة هو بالخارج عكس ذلك تماما.بل اساسيا للاختراق.يجب أن تجرى و بشكل مستمر التحقق عن طبيعة الاستفسارات وهوية أصحابها.هذا الإجراء يرفع من مستوى الحذر و التأهب لدى مستخدميك.ويلغي خرافة اسمها معلومات تافهة.
هندسة المصيدة:
بالطبع ليس كل المهندسين ذكورا .بل أحيانا إناث فاتنات وهذا هو الأخطر إذا تزامن مع موهبة إدارة دفة الحديث و سعة الاطلاع.و سرعة البديهة.فالتعامل اليومي و التكرار مع المعلومات يفقدها الحساسية و الأهمية .هنا على المهندس معرفة ذلك .فإذا جاء السؤال كان أمرا طبيعيا مما يفسح المجال لأسئلة أخرى والأفضل أن يتم بوتيرة بطيئة.. لازالة الشكوك ليكن هناك سؤال يدل على معرفتك ببواطن الأمور في المؤسسة. وهذا ما يمنحك الفرصة للوصول إلى مسؤولي الشركة الكبار تراتبيا أما طلبهم مباشرة خطأ فاحش.
رسالة متنبك:
كل معلومة لا تدل على نفسها تماما مثل أحجية الصورة المقطعة.ما أن تجتمع القطع حتى تتضح اللوحة.كذلك الأمر بالنسبة للمهندس الاجتماعي.يرى التركيبة الداخلية لكامل الشركة.هنا من الحكمة عدم إعطاء أي معلومات عن الشركة و موظفيهلاي شخص لم تثبت بالأدلة الكافية هوية المستفسر و مصداقية الطلب.
منع الخدعة:
تقع على عاتق الشركات مسؤولية توعية موظفيها و مدى المخاطر الناجمة عن إفشاء المعلومات و الإسرار.
إن الإدارة الكفوئة لسياسة امن المعلومات بالتزامن مع التوعية و التدريب المناسب .سيزيد من ادارك الموظفين على نحو كبير بالتعامل الصحيح مع معلومات الشركة.كما أن سياسة تصنيف البيانات ستعينك على تطبيق السيطرة الفعالة. حيث تعرف عن ماذا تكشف. بدون سياسة تصنيف البيانات كل المعلومات الداخلية يجب أن ينظر لها سري للغاية. هذه الخطوات تحمي شركتك.
المعلومات الغير مؤذية:
إن قسم امن المعلومات بحاجة لمعرفة الأساليب التي يتبعها المهندس الاجتماعي.ينطبق الأمر أيضا على الموظفين بان يأخذوا جانب الحيطة والحذر من متصل يبدو على دراية و معرفة بطرق سير العمل و الاجرات و التمعن مليا قبل إجابة طلبه و تحقيق ما يريد.هنا أيضا الشركة عليها مسؤولية تحديد الأساليب المناسبة للتحقق عند تعامل الموظفين مع أناس لا يعرفونهم. وتحديد الأدوار و المسؤوليات لكل منهم
رسالة متناك:
هناك قول مأثور وهو.حتى الأشخاص المصابون بالبار انوي لهم أعداء. علينا الافتراض أن كل شركة لها خصوم و أعداء
المهاجم أيضا الذي يستهدف البنية التحتية للشبكة بغرض المساومة على إسرار الشركة .
لا يجب إن يتوقف المرء عند إحصاء جرائم الحاسوب - انه الوقت المناسبُلتَقْوِية الدفاعاتِ الضروريةِ لتَطبيق السيطرةِ الصحيحةِ عبر سياساتَ أمنِ مدروسة بعناية.
؟؟ البار انوي هو مرض نفسي يشعر كل من يصاب به بالريبة تجاه الآخرين؟؟

القليل من الشركات يَعطي أرقامَ الهواتف المباشرةِ لمديرهم التنفيذي أَو رئيس مجلس إدارتِهُمْ أكثر الشركاتِ، مع ذلك، لَيسَقلقُلحول إعْطاء أرقامِ الهواتف إلى الأقسامِ والعاملين خصوصاً إلى شخص يَبْدو موظفا أو هكذا يبدو.
الإجراء المضاد المحتمل:
تطبيق سياسة تَمْنَعُ إعْطاء أرقام الهواتفِالداخليةِ للمستخدمين،المقاولون، المستشارون، الخطوة الأكثر أهمية بأهمية، تطوُير إجراء تدريجي لتَمييز الشخص المتّصل الذي يَسْألُ عن أرقام الهواتف حقاً مستخدمةُ.
اعتماد الرموزِ لمجموعات العمل والأقسام، بالإضافة إلى نسخ من الدليل المتَعلّق بالشركات (سواء النسخة المطبوعة، بيانات تَحْفظُ، أَو دفتر هواتف إلكتروني على إنترانت) أهدافَ متكرِّرة مِنْ المهندسين الاجتماعيين.
كُلّ شركة تَحتاجُ كَتبَ السياسة المَنْشُورة بشكل جيد على كشفِ هذا النوع مِنْ المعلوماتِ الوقاية يَجِبُ أَنْ تتضمَّن إبْقاء سجلَّ تدقيقِالذي يُسجِّل الحالاتَ عند كُشِفُ المعلومات الحسَّاسة إلى أناس خارج الشركةِ.

فصل 3

الهجوم المباشر

الطلب مباشرة:
العديد مِنْ هجماتِالهندسة الاجتماعية معقّدة، تَضْمن العديد مِنْ الخطواتِوالتخطيط المُتقَن، و مزيج من مهارة الاستغلال والتقنيات.
لَكنّي برأيي إن المهندس الاجتماعي الماهر يُمْكِنُ أَنْ يُنجزَ هذا في أغلب الأحيان هدفه بالهجوم المباشر الخالي من التعقيدات. فقط يَسْألُ بشكل صريح مباشر عن المعلومات المطلوبةُ.
أرادْ احد المهندسين معْرِفة رقم هاتف شخص ما الغير مُدرَج في دليل الهواتف.
هذه المعلومات محصورة بين موَظفي الشركة مع احد المهندسين الاجتماعيين بإجراء اتصال مع احد أقسام الشركة ويدعي انه من احد الشركات المتعاونة معهم.وهو عامل صيانة الكابلات وبحاجة لرقم معين و وما يتعلق بها لانجاز واجبه المرهق.
أنها من الطبيعة الإنسانية إن نثق بزملائنا. خاصة عندما يكون الطلب معقولا سهل التنفيذ.يقوم المهندس الاجتماعي باستغلال هذه النقطة لتنفيذ مأربه.
من مواصفات المهندس الاجتماعي الناجح . معرفته الدقيقة بالتفاصيل المتعلقة بالضحية سواء أكان فردا آم شركة.
رسالة متنيك:
بمثل هذهعلوماتِ المهرة لَيْسَ لهُمْ هواجسُحول الاتصال بالمسؤولون الحكوميون.المحليّون ليَتعلّموا حول إجراءاتِ تطبيقِالقانون.بمثل هذه المعلوماتِفي متناول اليدّ، المهندس الاجتماعي قَدْ يَكُون قادر على مُرَاوَغَة مستوى عمليات المراقبة الأمنية لشركتك.

قصّة المهاجمَ:
أعتقد دائماً بوبي والاس بأنّه من المضحِكَعند سؤاله للزبون لماذا يريد المعلومات إن الزبون مترددَ. في هذه الحالةِ يُمْكِنُأن يفكّر فقطً بسببين. ربما ممثلو بَعْض أقسام الشركةِالمهتمة َبشراء الشركةِ الهدفَ ومطلوب معْرِفة ما نوع وضعهم الماليالآن - خصوصاً كُلّماقد يريدون بقائه مخفيا عن أعين إي مشتري محتمل. أَو ربما مثّلوا بعض المستثمرون الذينَ فكروا أن هناك شيءُ مريبُحول طريقِة إدارة المال و اكتشاف سرقة مال من قبل المدراء التنفيذيين. رُبَّمَا زبونه أيضاً لَمْ يُردْ إخْباره السببَ الحقيقيَ لأنه إذا عَرفَبوبيأهمية المعلومات لربما طلب مالا أكثر لإنجاز العمل.
هناك الكثير مِنْ الطرقِ للولوجلملفات الشركةِالأكثر سريةً. بوبي صَرفَبِضْعَةأيام يُفكّر في الخيارات المتاحة أمامه و فحص ما استقر عليه من خطة عمل. اشترى هاتف خلوي . اتصل مع الرجلِالهدف ، قدم نفسه انه مِنْقسم رعاية الزبائن الشركةَ، بهذه الطريقة يصل لجهازالضحية يزرعفيه كود ليطلب الضحية المساعدة مرة أخرى عن طريق التروجان أو أحصنة طروادة.

قصّة كريج:
كان كريج كفئ كبائع في شركة تقنية، بعد فترة بَدأَ بإدْراك بأنّه كَانَ عِنْدَهُ مهارة لقراءة الزبون،بفَهْم أين الشخص يقاوم وأكتشف بَعْض الضعفِو قلة المناعة الذي جَعلا الأمر سهلاً لإتمام البيعِ فكّرْ بشأن الطرقِ الأخرى لاستعمال هذه الموهبةِ، مما أوصله لمجال ذو فائدة أكثر بكثير من عمله كبائع:
وهو التجسس الصناعي.هذه كَانَت مهمة مثيرة.الآن أصبح بالإمكانالسفر بيسر إلى هاواي. أَو رُبَّمَا تاهيتي.الرجل الذي استأجرني، هو لَمْ يُخبرْني من هو الزبونَ، بالطبع، لَكنَّه أعتقد إحدى الشركات التي أرادتْ اللحاق بالمنافسة بسرعة كبيرة،
القفزة السهلة:
تقمصت شخصية أخرى للمهمة.. الشركة دُعِيتْ جيمي ميد للصناعات الدوائية. مَا سَمعَ عنها، لَكنَّكانت من كبريات الشركات مصنفة ضمن اكبر 500 شركة بأميركا - مما يسهل أداء المهمة فمن المحال كشركة عملاقة إن إي موظف يعرف كل العا ملين بالشركة.زبوني أرسلَ لي فاكسا، فيه بعض المعلومات عن منتج الشركة الهدف الجديد.. . كَانَ عِنْدي شيءُ واحد احتاجه للتخطيط والآن أبدا، اسم المُنتَج الجديد.المشكلة الأولى : تَحْصلُ على أسماءِ الناسفي الشركةِ التي عَملتْالمنتج أَو قَدْ يَحتاجُ لرُؤية التصاميم لذَا اتصلت مع مقسم الشركة وقُلتُ، "أنا موَاعَدَ أحد الناسفي قسم التخطيط ولا أَتذكّر اسمَه الأخيرَ. لكن اسمَه الأولَ بَدأَ بحرف س . " قالَت الموظفة، "عِنْدَنا نَبّال سك.م ديفيد سن." انتهزت هذه الفرصة الغير متوقعة . "لأسالها أيهم يعمل في مجموعة STH 100؟ "هي لَمْ تَعرفْ، لذا أنا فقط اخترت نَبّال سكوت عشوائياً، وهي اتصلت به.عندما أجابَ، قُلتُ، " ، هذا مايك، في غرفةِالبريد. نحن عِنْدَنا عقد هنا لمشروع ِ-100 .هل من فكرة لديك لمنْ يَجِبُ أَنْالجأ؟
"أعطاني اسمَ رئيس المشروعَ،جيري ميندل. اتصلت به لكن رسالةَ بريده الصوتي قالتَ بأنّه سَيَكُونُ في إجازة حتى الثالث عشْر،وأي شخص بحاجة لشيءَ في هذه الأثناء يَجِبُ أَنْيتصل مع ميشيل على 9137. اتصلت معها وقلتُ، "هذا بيل توماس. جيري أخبرني أنك جاهزة ويريد المواصفات جاهزة ويريد فريق عمله للمراجعة. إذا

بدت مرتابة سأخبرها إنني أودي معروفا لجيري بناءا على طلبه، هكذا حصلت على ما أريد من معلومات بدون إثارة الشبهات. جيري قال بأنّك يُمْكِنُ أَنْ تَعطيني قائمة عناوين البريد الإلكتروني لفريق التطويرِ،إياك وزيارة المباني التي تخص الهدف ما لم تكن مضطرا.

الاختراق:

تبقى لدي خطوة واحدة عظيمة لدخول حاسوب الشركة.

لَكنَّ لا زلت بحاجة عدة معلومات.تظاهرت إنني حد الموظفين الجهلة بالحواسيب و احتاج للمساعدة. حصلت على بيانات و إجراءات الدخول لحاسوب الشركة من الخارج كان الموظف متعاونا وما قام بإعطائي كأنه أمر روتيني عادي.

تفكيك الباسوورد: الكثير من الهراء عن حماية الباسوورد. السبب طبعا الافتراض الوهمي إنّ العمليةَ غير قابل للنقض؛ مع الاعتقاد انه لا يمكن إعادة صياغتها

تفكيك الباسوورد:

دخلت من حسابِ الضيفَ،دخلت الآن إلى حاسوبِواحد، الذي يعمل على نسخة قديمة مِنْ نظامِ تشغيل اليونيكسَ تحت اليونيكسِ.

نظام التشغيل يعالج ملف كلمةِ سر بشيفرة طويلة كُلّ شخصِ مخول لدُخُول ذلك الحاسوبِ ملف كلمةَ السر يَحتوي طريقة واحدة للتفكيك(إحدى طرقِ التشفيرِ المنيعة) كُلّ كلمة سر مستعملِ. مَع التفكيك أحادي الاتجاه كلمة سر فعلية مثل، رأي،"justdoit" سَيُمثّل مِن قِبل التفكيك في الشكلِ المشفِّر؛ في هذه الحالةِ، التفكيك سَيُحوِّل باليونيكسِ إلى ثلاثة عشرَ خانة حرفية أو رقميةِ.

حوَّل بيلي بَعْض الملفاتِ إلى الحاسوب، وعرف نفسه بتَزويد اسم المستعمل وكلمة السر. النظام دقَّق كلمةَ السر المدخلة ، وبعد ذلك

تُقارنُ النتيجةُ بكلمةِ السر المشفَّرة (المفككة) المتضمنة في ملف كلمةِ سر؛ إذا تم التطابق يتم إدخاله لأن كلماتَ السر في الملفِ المشُفَّر، الملف بنفسه جُعِلَ متوفرا إلى أيّ مستعمل طبقا للنظريةِ القائلة لا يمكن كسر الشفرة.

اعتمادا على ما حصلت عليه سابقا القوائم البريدية لفريق التطوير. ستيفن r، كَانَ عِنْدَهُ حسابُ حالياً على الحاسوبِ بكلمةِ السر "جانيس."في الوقت المناسب إذا تم ذلك سيوفر الكثير من العناء و الوقت.حتى لو كشف اختراقي هذا لقوائم البريدية كافية و مفيدة.حملت ما أريد من برامج التطوير لمشروعهم. لأرسله لموقع في الصين بدون إثارة الشبهات .

الهبوط الميت:

مكان لتَرْك المعلومات حيث من غير المحتمل أنْ يَجِدُه الآخرون. في عالمِ الجواسيسِ التقليديين، بغاية الخطورة .ألان وبتوفر الانترنيت أمر متبع من قبل الهاكرز.

تَحليل الخدعة:

بالنسبة للرجلِ المَدْعو كريج ، أَو أي واحد مثله ماهرِ على حد سواء في -السرقة لكن لَيسَ دائماً- الهندسة الاجتماعية، التحديَ روتينيًا تقريباً. هدفه كَانَ أَنْ يُحدَّد مكانَ الملفاتَ ويُحمّلها.المخزنة في حاسوب الشركة، أنجز العمل بيسر رغم أنها محمية مِن قِبل برنامج حماية وكُلّ تقنيات الأمن المعتادةِ.

تَظَاهُر بصفة شخص ما مِنْ غرفةِ البريد و الإمداد و متظاهرا أنه بانتظار عرض مهم عطَّل كريج أيّ شكوك بالإدِّعاء بأنه كَانَ يرَدّ على رئيس المجموعة.-الذي هو بإجازة ـ،لم يكون هناك طريقة للتثبت من صدقيه أقواله. كما لا يمكن إن يتحمل الموظفون -حسبما ارتأوا- عاقبة عدم التعاون و المساعدة بغيابه . مرةً أخرى، هنا مثالُ عن شخص تدفعه الرغبة القوية ليكون عضوا نشطا، مما يكونون عرضة أكثر للخداع إرسال البيانات بالفاكسُ جنبه خطر دُخُول البنايةِ. موظفو الاستقبال يختارونَ عادة لشخصياتِهم السَاحِرةِ وقدرتِهم لخلق انطباع جيد. -لكنهم أيضا عديموا الخبرة بقيمة و اهمية المعلومات .

رسالة ميتنيك:

أولوية كُلّ شخص إنجاز العمل. تحت ذلك الضغطِ، تَأْتي التطبيقات الأمنية بالمرتبة الثانية في أغلب الأحيان أَو تُهملُ هذه إحدى نقَاط الضعف التي يعتمد عليها المهندس الاجتماعي .و ضعف الحماية الأمنية التقنية في الشبكات الداخلية.

مَنْع الخدعة:

تَتضمَّن إحدى أقوى خُدَعِ المهندس الاجتماعي قلب الموازين لصالحه . يثير المهندسُ الاجتماعي المشكلةُ،وبعد ذلك يَحْلُّ المشكلةَ بطريقةَ سحرية، يَخْدعُ الضحيَّة للدخول إلى أكثر أسرار الشركةِ حماية.

تعلّمْ، تعلُّم، و تعلَّم. . .

هناك قصّة قديمة حول زائر إلى نيويورك أوقف رجلا في الشارعِ وسأله، " كَيفَ أَصِلُ إلى قاعةِ كارنيجي للموسيقى؟ " أجابه الرجل "التمرين التمرين التمرين." لذا كُلّ شَخص عرضة لهجماتِ الهندسة الاجتماعية. و دفاع الشركةِ الوحيدِ الفعَّال تعلَّيم وتدرَّيب مستخدميك، بمنحهم هذه الممارسة ليكونو قادرين على اكتِشاف

المهندس الاجتماعي. وبعد ذلك يَستمرُّ بتَذكير الناسِما تَعلّموافي التدريب، فالكل عرضة لان أن ينسى.لأنه من سجايا الإنسان الرغبة في الثقة بالآخرين. لكن كما يقول المثل الياباني -البزنس حرب- فإعمالكلا يمكنها تحمل تخفيض مستوى الوقاية.
سياسة الأمنِالمتعلّقة بالشركاتِيَجِ بُأَنْ تحددالأساليب الملائمة وغير الملائمة بشكل واضح.الأمن مستويات.
الموظفون عِنْدَهُمْ أدوارُ متباينةُ عادة
و مسؤولياتَ وكُلّموقع له نقاط الضعف مترابطة. يَجِبُ أَنْ يَكُونَ مستوى أساسي مِنْالتدريب لكُلّ شخصفي الشركةِ عليه اجتيازه، كل حسب عمله و موقعه والتزام ببَعْض الإجراءاتِالتي سَتُقلّل الفرصةَ لاستغلالهم. الناس الذين يَعْملونَ بالمعلوماتِالحسّاسة أَو في مواقع الثقةِ يَجِبُ أَنْ يتلقوا تدريبات متخصصة إضافية.

استمرار بسلامةِ المعلوماتِالحسّاسة
عند اقتراب احد الغرباء من الناس عارضا المُسَاعَدَة. هم يَجِبُ أَنْ يَستندوا على سياسةِ الأمنِالمتعلّقة بالشركاتِالمصممة لتامين الاحتياجاتالأمنية، حجم، وثقافة شركتِكِ

مُلاحظة:
شخصياً، لا أَعتقدُ بسلامة التبادل لكلماتِالسر. على الشركات أن تمنع هذا و بحزم.و العمل لتأسيس ثقافة أمنية خاصة بها. إدخال أوامر غير مألوفة تغيير إعدادات برنامج فتح ملحق بريدي أو تنزيل برنامج لم يدقق. عدم التجاوب مطلقا مع إي غريب يطلب الاطلاع على البيانات.من الطبيعي نسيان ماتعلمناه الحل هو التدريبات الدورية.
لاتظن أبدا إن المهندسين يحتاجون لخدع مفصلة معقدة .لأنه من المحتمل التعرف إليهم قبل انجاز هدفهم. فيكون الهجوم قصيرا فعالا مثل الكر و الفر.
هجوم بغاية البساطة و لا أكثر.
عليك بتنمية ما يسمى غريزة المهندس مثل غريزة الصياد . كيف تجعل الشخص في الطرف الأخر يتعاون معك.
منع الخدعة:إحدى المسائل التي يجب إن تكون ضمن برنامج التدريب : معرفة المتصل أو الزائر بأسماء بعض الموظفين أو إجراءات الشركة أو أساليبها
لا يعني بالضرورة انه من يدعي. و لا يبرهن قطعا كشخص مخول ومسموح له بأخذ معلومات الشركة الداخلية الخاصة.و الولوج إلى أنظمة الحواسيب والشبكة.فالتدريبات الأمنية بحاجة لتأكيد: عند وجود شك أو ارتياب عليك بالتحقق فورا وبدون تأخير.لان الدخول لبيانات الشركة هو أمر محصور بفئة معينة سلفا و محددة.السياسة الأمنية يجب إن يعرفها كل الموظفون بغض النظر عن الموقع.المهندس الاجتماعي يركز هجومه على قسم خدمة الزبائن لأنه الرابط الأضعف.. لمحاولات الهجوم والخداع فهم طبعا. الموظفون الجدد .لقلة خبرتهم وسهولة خداعهم. لذلك على أي شركة تريد زيادة مناعتها وتحصينها التغلب على نقطة الضعف هذه.

الفصل الرابع

بناء الثقة :
ما يجري من عمليات خداع للآخرين يقودنا نحو الاعتقاد التالي.إن كل موظف أو عامل .مستوى الغباء لديه مرتفع مستعد و متلهف لنشر كل إسرار العمل التي بحوزته.المهندس الاجتماعي يدرك إن هذا غير صحيح. لماذا اذاً هجومه ناجح على نحو مبهر؟
السبب ليس غباء الناس أو افتقادهم للحس السليم. لكن كوننا بشرا عرضة للخداع للثقة بالشخص الغير مناسب.إذا استغل بطريقة معينة.
يتوقع المهندس الاشتباه و حتى المقاومة ذكائه وخبرته يقلبان القلق إلى ثقة .المهندس الماهر يخطط لهجومه مثل لعبة الشطرنج.حيث يقوم بتهيئة نفسه إن المستهدف قد يمطره بوابل من الأسئلة.ليكون مستعدا للإجابة وبشكل صحيح.من أساليب المهندس المتبعة بكثرة . إشاعة جو من الثقة مع الضحية.
كيف له ذلك؟
يجب إدراك القاعدة التالية .الثقة أساس الخداع:ما أكثر ما يستطيع القيام به المهندس الاجتماعي ليؤدي مهامه بكل سلاسة ودون إثارة الشكوك أو تغيير
غير متوقع .من السهولة بمكان على المهندس كسب ثقة الضحية حالما يتم ذلك .يبدأ العد التنازلي.لانجاز الهجوم بنجاح.إن بناء الثقة احد أهم العوامل للنجاح عليك التفكير مليا هل تعرف الشخص الذي أمامك هل هو من يدعي.علينا أن نتعلم الملاحظة و التفكير و أحقية السؤال عن طلب ما.
تمعن بموقفك .عند سؤال شخص غريب منك رث الثياب من المحتمل أن ترفض استقباله أو حتى الإجابة عن سؤاله. لكن ماذا لو كان أنيقا مهذبا محترما.ستكون اقل اشتباها به. الانطباع الأول كثيرا ما يكون خادعا.فالثقة

تتشكل هنا حسب مظهر الطرف المقابل لنا و هذا خطا فادح . فالشك له فوائده .فهي تمنعنا من الانزلاق إلى خسائر قد تكون مكلفة .علينا تذكر مقولة كانت تقال لنا باستمرار و نحن صغار لا تثق بالغرباء.إن مجرد السؤال عن أيميل زميلك أو حتى تفاصيل صغيرة عن احد زبائن شركتك حتى لو كان السائل احد زبائن الشركة. كفيل بقرع أجراس الإنذار.معظم الناس يبحثون عن الصفقة الأفضل إما المهندس الاجتماعي فانه يبحث عن الطريقة الأحسن لانجازها على أحسن ما يمكن. الشركات تطلق أحيانا حملة دعائية لأحد منتجاتها بطريقة من الصعب إن تدعها تمر مرور الكرام .المهندس ينظر للعرض كيف له الاستفادة بالحد الأقصى من العرض.

تحليل الخدعة:

من الطبيعي أن يكون هناك قبول من قبل الناس إذا كان الطرف الأخر زميلا أعلى رتبة ويعلم بإجراءات الشركة. المهندس الاجتماعي البارع لا يتوقف لحظة للتأمل في كيفية اختراق قواعد البيانات. لأنه ببساطة من الصعب مقاومة شخص يتكلم بلطافة و إقناع .

منع الخدعة :

ما الخطوات التي يمكن إتباعها في شركتك للتقليل من إمكانية استغلال المهندس . الغريزة الطبيعية لدى مستخدميك الثقة بالآخرين.

بعض الاقتراحات لحماية زبائنك .في هذا العصر الالكتروني العديد من الشركات تحول جاهدة التمسك بزبائنها وهم يشترون منها نسخة من أرقام بطاقته

للأسباب التالية: تكفي الزبون عناء تزويد بيانات بطاقته الائتمانية في كل مرة يشتري بها هذا العمل يجب أن يلغى .أما إذا اقتضى العمل على ذلك الاستمرار بحفظ نسخة الإجراءات بحاجة أن يتزامن معها . ولا تتوقف الإجراءات على التشفير أو مراقبة الوصول الأمنية . الموظفون بحاجة للتمرين على أساليب الغش لدى المهندسين. فزميلك بالعمل والذي أصبح صديقك على الهاتف والذي لم تلتق به ربما ليس ما يدعي , وانه بحاجة لمعرفة كيفية الدخول لبيانات الزبائن الحساسة .

رسالة متنبك :

يجب على الكل الحذر من أساليب المهندس الذي يجمع المعلومات عن هدفه بقدر ما يستطيع , ثم يستخدمها لاكتساب الثقة كأنه من أهل البيت ثم يقوم بهجومه المدمر .

ثق بتعقل :

المعلومات الحساسة جدا لا يدخلها فقط أناس مثل المبرمجون أو مختص الأبحاث والتطوير وهكذا دواليك. فكل من هو بموقع دفاعي ضد الهجمات بحاجة للتهيئة لحماية ممتلكات المؤسسة .لهذا السبب يجب إجراء مسح شامل وعام عن أصول ممتلكات الشركة المعلومات الحساسة والقيمة ومعرفة ما الأساليب التي يمكن أن يتبعها المهاجم للاستحواذ عليها . التدريب الملائم للموظفون المخولون للدخول إلى تلك المعلومات يجب أن يعتمد على الإجابة عن الأسئلة التالية :

عند ما يطلب منك أي شخص بعض المعلومات والمواضيع أو أن تؤدي له عملا على حاسوبك .هل ما أقوم به هو لصالح أعداء مؤسستي , هل من الممكن أن تؤذيني أو تؤذي شركتي , هل أنا مدرك للعواقب المحتملة عند قبولي بالدخول لحاسوبي لا نريد من خلال هذه الأسئلة الاشتباه بكل البشر الذين نلتقي بهم مصادفة الحذر ضروري وواجب , الحكمة تقتضي بفحص حواسيب الشركة بشكل دوري وخاصة الانترانيت .

الفصل الخامس

الرجاء مساعدتي

نكون بغاية الامتنان عندما نبتلى بمصيبة ويأتي شخص ما ماهر مطلع وخبير ليقدم لنا يد المساعدة المهندس يدرك ذلك و يعرف كيفية استغلال ذلك لصالحه .وما يعرفه أكثر كيف يسبب لك مشكلة ليجعلك بعدها ممتنا له عندما يحلها لك . ليقوم بعد ذلك باستغلال امتنانك له لاستخراج بعض المعلومات أو خدمة صغيرة. والذي سيترتب جراء ذلك عليك أو على الشركة أسوء النتائج أو لربما لا تعرف كيف فقدت شيئا قيما.

حصان طروادة :

برنامج يحتوي على اكواد ضارة صممت للإضرار بحاسوب الضحية أو ملفاته . أو للحصول على معلومات من حاسوبه وشبكته .بعض أنواع التروجان مصممة للاختباء في ملفات النظام وتتجسس على كل ضغطة مفتاح أو عمل تؤديه على حاسوبك , انه حتى يقبل الأوامر عبر الانترنيت لأداء بعض المهمات كل هذا بدون ملاحظة الضحية لذلك . هذا ليس كل شيء بإمكانه العودة بأي وقت للبحث خلال رسائل الايميل والمذكرات الخاصة لمدراء الشركة . يقوم بالبحث عن كل ما هو مهم أو يحوي معلومات قد تكون مؤثرة.

تحليل الخدعة :
المهاجم يسرع الويب لإقناع الضحية لديه حل للمشكلة التي يعاني منها .في الواقع هي غير موجودة لكن ستحدث حتما لأنه سيقوم بذلك ليقدم نفسه على انه من لديه الحل هكذا يكتسب المصداقية التي تستند لأوامر تقبل أداء بعض الوظائف المعينة أو تشغيل البرامج . المهاجم الذي يستغل الثغرات الضعيفة تقنيا أو بإمكانه الدخول إلى صفحة الأوامر.

الهندسة الاجتماعية العكسية :
هجوم الهندسة الاجتماعية في وضع يكون فيه الضحية يعاني من المشكلة التي جهزها له المهاجم ليتصل بالمهندسين طلبا للمساعدة .هناك شكل آخر من الهندسة الاجتماعية المعكوسة : الهدف يتعرف إلى المهاجم و يستعمل مبادئ التأثير النفسي لإمداده بالمعلومات قدر ما يمكن من المهاجم لتكون أعمال الضحية بأمان.
رسالة متنبك:
إذا طلب منك غريب أداء خدمة مقابل خدمته لا تقدم على ذلك بدون التفكير مليا حول طلبه.مثل هذه الخدع يقوم المهاجم باستثمار نقص معرفة الضحية بالحواسيب.لذلك كلما كان الضحية أكثر معرفة وإدراكا كلما ازداد الشك لديه وانه موضع استغلال خبيث.وما اسميه العامل الحاسوبي الحاسم.
الشخص ذو معرفة قليلة بالحواسيب واجراءاته على الأغلب يكون أكثر امتثالا و استجابة للانجرار نحو الفخ.-
فقط قم بتنزيل هذا البرنامج-
لعدم وجود فكرة لديه عن المخاطر المحتملة التي يمكن أن يواجهها جراء ذلك .و الأدهى من ذلك ألا يكون مدركا لأهمية و قيمة المعلومات الموجودة في حاسوبه.
مساعدة صغيرة لفتاة؟ الموظفون الجدد هدف دسم للمهاجم لا يعرفون الناس بشكل كاف .انتفاء الخبرة الكافية .ولغاية خلق انطباع حسن عنهم فهم متلهفون لإبداء التعاون و الاستجابة في عملهم .ماذا لو اتصلت فتاة ذات صوت خلاب موحية إنها من احد أقسام الشركة طالبة المساعدة أو مباشرة ما سيكون رد فعلك و أنت جديد العهد بالعمل.
تحليل الخدعة:
أكثر المعلومات التي يريدها المهندس من الموظف بغض النظر عن هدفه النهائي مؤهلات الضحية وما ما هو مخول به لدخول بيانات
الشركة .عن طريق بيانات الضحية تتحدد ما سيخترقه قبل السماح للموظفين الجدد بالدخول إلى أنظمة حواسيب الشركة يجب تدريبهم بالشكل الكافي خاصة عدم إفشاء كلمات السر لأي كان حتى لو كان زميلك بالعمل.
ليس آمنا كما تظن :
الشركة التي لا تبذل جهودا كافية لحماية معلوماتها و بياناتها .عرضة للمخاطر .هناك حقيقة أخرى انه مع توفر الحماية لأصول لشركة لا يعفيها من
مما هو مخبأ من مخاطر.

؟؟ أرجو أن لا نكون قد اطلنا عليكم وموعدنا السبت القادم حيث يبدأ التشويق شيئا فشيئا؟؟