بسم الله الرحمن الرحيم

أهمية التوعية الأمنية Security Awareness Importance

مقدمة :

سوف نتحدث في هذه الورقة عن التوعية الأمنية وأهميتها وأهدافها وبعض النقاط المتعلقة بها والمفاهيم التي يجب توعية وتثقيف جميع العاملين بها من حيث الوعي الأمني للأنظمة الحاسوبية في أي منظمة.

تعنى التوعية الأمنية بحماية الأنظمة والبرامج من خلال وعي مستخدم الحاسوب أو النظام بأهمية حفظ معلوماته وبياناته والحرص عليها وتهيئة الأجهزة الأمنية والبرامج اللازمة لذلك.

الأهداف:

1- تثقيف العاملين بأهمية الأمن في المنظمة وتدريبهم على ذلك.
2- تطوير إطار أمني للتعامل مع المخاطر بجميع مستوياتها: العالية والمتوسطة والمنخفضة.
3- تهيئة العاملين للتعود بمفهوم الأمن الشامل وسرية المعلومات.[5][2][1][9]

المخاطر (الهجوم):

- إساءة استعمال المصادر والتي قد يستخدمها المهاجم في الهجوم على النظام أو الأنظمة الأخرى في المنظمة.
- فساد البيانات – إظهارها – مسحها.
- تعطيل الخدمة DoS.
- تتبع الشبكة واقتناص المعلومات المرسلة غير المؤمنة عن طريق البريد أو تراسل الملفات أو غيرذلك.
- سرقة الأجهزة المحمولة.
- الهندسة الإجتماعية:

من ضمن الأقوال الخاطئة من قبل الأشخاص غير المثقفين أمنياً هو أن (البيانات ليست مهمة لهذه الدرجة) وهؤلاء هم الأكثر عرضة للهجوم من خلال الهندسة الإجتماعية.

مفاهيم إمنية:

هناك بعض المفاهيم الأمنية التي يجب أن تطبق بحيث يكتمل مفهوم الأمن الشامل من قبل العاملين وأجزاء المنظمة الأخرى: – توحيد البنية التحتية الأمنية – تطبيق السياسات والإجراءات للأنظمة الحاسوبية.

- التدريب التوعوي والتثقيف الأمني لجميع مستخدمي الأنظمة بحيث يكون كل شخص مثالاً للآخرين على المستوى الأمني. – الحلول التقنية(الجدران النارية، أنظمة تحديد التطفل ..).

ويمكن أن تعمل هذه المنظومة جميعها مع بعضها البعض على حسب مستوى المخاطر، بحيث يتوازن المستوى الأمني مع رسالة المنظمة.

بعض الأخطاء المسببة للثغرات الأمنية بسبب قلة الوعي :

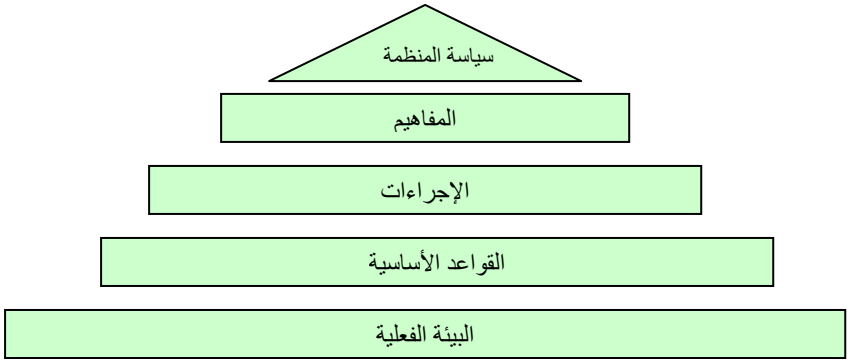
1- تكليف الأشخاص غير المتدربين بالعمل على النظام الأمني وتعديله.
2- عدم فهم العلاقة بين أمن المعلومات وفائدتها لعمل القطاع أو الشركة.
3- عدم إدراك قيمة المعلومات الخاصة بالمنظمة.
4- تجاهل المشاكل البسيطة أو الملاحظات الأمنية مما يؤدي إلى مشاكل أكبر وفقد للبيانات وبالتالي إلحاق خسائر مالية كبيرة للمنظمة.
5- تجاهل متابعة عمل التحديثات وآخر التعديلات على الأنظمة بحجة عدم أهميتها.

أهمية الحماية من خلال كلمات المرور :

يجب على مسئولي الأمن نشر الوعي لدى العاملين بأهمية حفظ المعلومات المهمة من خلال المحافظة على كلمات المرور ولماذا تحفظ بعيداً عن أنظار المتطفلين، وكيفية حفظها، بالإضافة إلى ضرورة تغييرها كل فترة حتى لاتكون هدفاً للمهاجمين.(Password Guessing).[6]

ماالهدف من وجود سياسات أمنية؟

وجود السياسات الأمنية التي يجب على الموظفين أو العاملين اتباعها، يرجع السبب في ذلك لأن أمن المعلومات أصبح جزء رئيسي وضروري لإنجاح عمل أي منظمة وليس كناحية تقنية فقط؛ فعند إلتزام الجميع بهذه القواعد وتطبيق المفهوم الأمني على كافة الأنظمة يرتفع مستوى الأمن وزيادة السرية للمعلومات وبالتالي تحقيق أهداف المنظمة. إذا تبدأ السياسة من قمة الهرم لدى المنظمة.



شكل (1).[10]

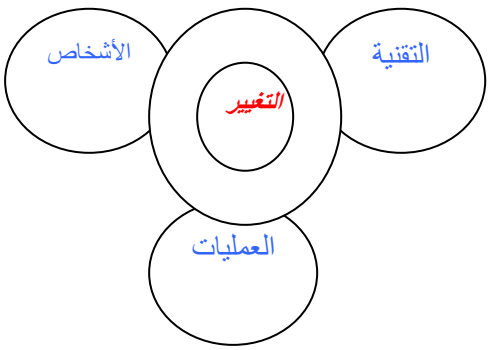
- يجب أن تتوفر جميع هذه النقاط لدى المنظمة بالإضافة إلى التدريب الأمني للعاملين

برامج التدريب:

إن الهدف هو تعريف معايير معينة من أجل التدريب الأمني وبرامج التوعية لتثقيف الموظفين بالمتطلبات اللازمة لحماية حالة البيانات ومصادر تقنية المعلومات ومن ثم تطوير المعرفة والمهارات الضرورية لحاجة أمن تقنية المعلومات.

علاقة سياسة التغيير بأجزاء المنظمة:

قد يتطلب الأمن المعلوماتي في المنظمة إلى تغيير في أحد العناصر السابقة : السياسات، الإجراءات، المفاهيم وغيرها؛ أو تغيير البنية التحتية للعتاد وأنظمة التشغيل؛ وذلك بهدف حماية المعلومات أو زيادة الأمن وحجب المخاطر المتوقعة من قبل المهاجمين والمتطفلين.



شكل (2) - [2]

حساسية المعلومات المالية:

- تعتبر المعلومات المالية من أهم المعلومات التي يجب المحافظة عليها في المؤسسات المالية وعدم إعطاء فرصة للمتطفلين في اقتناص تلك المعلومات، وإليك هذا الخبر عن أهمية التوعية الأمنية:

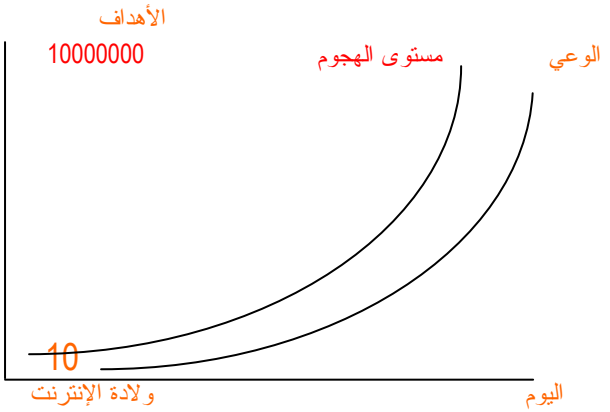
- تلقت شرطة كاليفورنيا العديد من البلاغات خلال الأيام الماضية التي تفيد اتصال أشخاص بطلاب جامعة كاليفورنيا عبر هواتفهم الجوالة يطلبون منهم بياناتهم الشخصية خاصة أرقام حساباتهم في البنوك، حيث يدعون أنهم ممثلون لبعض الشركات التي يمكنها تأمين حساباتهم عبر الإنترنت بالإضافة إلى حماية البيانات الشخصية المحفوظة على الحاسبات المنزلية الخاصة بهم .

وكانت السلطات الأمنية قد تلقت أول بلاغ من شاب يدعى مايكل منجويا (20 عاما) ثم توالت البلاغات مما دعا المسؤولين الأمنيين بالجامعة بالاشتراك مع وزارة التربية والتعليم هناك إلى إطلاق حملة توعية للطلاب لتحذيرهم من تلك الأفعال وقاموا بتسمية الحملة (ثقافة التسويق الهاتفي) وتضمنت الحملة عدة تعليمات مثل (عليكم حماية بياناتكم الشخصية مع ضرورة حجبها عن اللصوص والأشخاص غير الموثوق بهم) وفي بيان صحفي للمفتش العام للأمن ويسمى جون بي هاجينس قال: (على الطلاب أن لا يتركوا اللصوص يسرقون هوياتهم الشخصية .)

وأضاف رئيس الجامعة أن الطلاب عديمي الخبرة المالية يكونون أكثر عرضة لسرقة هوياتهم مشيرا إلى أن معظم طلاب الكليات يجهلون الطرق التي يمكنهم من خلالها حماية بياناتهم الشخصية وكان عدد من الخبراء التقنيين والأمنيين المشاركين في حملة التوعية قد أصدروا عدة ملاحظات وطالبوا الجميع بالالتزام بها لحماية أنفسهم ومنها أهمية حماية أرقام بطاقات الائتمان مع ضرورة الالتزام بعدم تدوينها على بعض الكتب المدرسية أو المذكرات والمفكرات التي قد يحملها الطلاب في حقائبهم ونصحوهم بمحاولة حفظها في ذاكرتهم كما طالب الخبراء بالابتعاد عن استخدام التواريخ التقليدية ككلمات سر للحاسبات الخاصة بهم سواء في الجامعة أو المنزل التي يسهل توقعها من قبل اللصوص مثل تواريخ الميلاد .

وأضافوا أن الطلاب يجب أن ينتبهوا إلى الأوراق التي تتعلق بالمعاملات المالية مع ضرورة تمزيقها قبل إلقائها في سلال المهملات بالإضافة إلى عدم التصريح بالبيانات المالية من خلال الهواتف أو الإنترنت إلا بعد التأكد من شخصية طالب تلك البيانات مع أهمية استخدام برامج الحماية على الحاسبات الخاصة بهم سواء داخل الحرم الجامعي أو بالمنازل خاصة للذين يتركون حاسباتهم على اتصال بشبكة الإنترنت طوال الأربع والعشرين ساعة وحذر مدير أمن الجامعة من إتاحة بيانات الطلاب الخاصة على الحاسبات التي لا تتمتع بحماية مطلقة مشيرا إلى إمكانية تعرضها للسرقة كما حدث خلال الشهور الماضية، وأضاف أن حاسبات الكليات والجامعات تعد (منجم ذهب)للصوص بما تحتويه من بيانات خاصة بالطلاب وأعضاء هيئة التدريس، وكانت السلطات الأمنية قد أعلنت أن أحد الأقراص الصلبة الذي يحتوي على الكثير من البيانات الشخصية الخاصة بالعاملين في الجامعة قد تعرض للسرقة في أوائل شهر سبتمبر الماضي مما أثار حفيظة الكثير من المسؤولين والتحذير بضرورة تشديد الحراسة على تلك الأجهزة.

علاقة التزايد في الهجوم مقابل مستوى الوعي:



شكل(3)[11]

الخبرة الأمنية:

قد تستعين المنظمة بشركات أخرى أمنية للتدريب ورفع مستوى الحس الأمني لموظفيها وزيادة وضع أمن طبيعي وتقني لدى الشبكات المحلية والمتصلة بالإنترنت. لكن يبقى النظر منصباً على ذوي الخبرة الأمنية للإستفادة منهم ونشر الوعي الأمني لدى بقية الأقسام والفروع.

الخاتمة :

نستخلص مما سبق التالي:

- ضرورة إدراك أهمية وقيمة المعلومات في جميع الأنظمة بما فيها الحاسوبية.
- أن مفهوم التوعية الأمنية ليس مجرد تدريب فقط.
- التوعية الأمنية معني بها الجميع: -حماية وأمن كلمات المرور.
  -أمن المنشآت والأفراد.
  - حقوق البرامج والخصوصية.
  -هجمات الهندسة الإجتماعية....الخ.

References :

[1] C. Office of Technology, "*Security Awareness Newsletter*", COT Division of Security services, October 2004, volumeII, Issue 4.

[2] Commonwealth Office of Technology,http://gotsource.ky.gov/dsweb/get/document-40461/SA+NewsLetter, , published by the COT Division of Security Services, October 2004, Volume II, Issue 4

[3] M. CIAMPA ,"Security+ guide to network security fundamentals", 2nd edition, Canada: Course Technology, 2005.

http://www.al-jazirah.com.sa/digimag/02012005/wr37.htm[4]

[5] A. Mohammed,"*Aljazirah Office : Security Awareness*" ,Cairo, 2002.

[6] security focus, www.securityfocus.com/archieve/132/353712, protecting password, message to security management, US-CERT securityawareness tips, Feb 12 2004.

[7]Semantic Corporation, April 23 2005, http://securityresponse.symantic.com/avcenter/security/content/security.articles/corp.security.policy.html.

[8] azgita gov, April 5 2004, http://azgita.gov/policies_standards/html/p800_s895_security_trng.htm.

[9] Insight company, april 23 2005, http://www.insight.co.uk/training/training.htm

[10]http://securityresponse.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html

[11] *Infosec corporation*, april 23 2005,http://www.infosec.co.uk/ExhibitorLibrary/131/ProactiveNetworkSecurity.pdf, Circle Proactive Network Security.