بسم الله الرحمن الرحيم

أساسيات أمن المعلومات

مكونات البحث:

المقدمه:

سوف نتطرق في هذا البحث بأذن الله لأساسيات أمن المعلومات في المنظمه وكيفيه بناء البنيه التحتيه لأمن المعلومات والسيطره على الاخطار الممكنه والاجراءات اللازمه للوصول والرقي بالمنظمه لنظام أمني متكامل في ظل وجود تفاعلات واتصالات اللازمه بين جميع الوظائف المختلفه والاخذ بنصائح الاستشارين في أمن المعلومات والتعاون بين الاجهزه المختلفه في المنظمات المختلفه, تشريع الاجراءات اللازمه والتأكد من تطبيقها..ونتطرق ايضا الى اهميه وجود أمن للموظفين في المنظمه والحرص على تدريبهم وتوعيتهم من الاخطار المحيطه بهم من نصب واحتيال وسرقه معلومات تتعلق بأمن المنظمه.
ايضا نعطي نبذه عن كيفيه تحقيق بيئه أمن مناسبه وذلك بعمل عدد من الاجراءات اللازمه لمنع الدخول الغير مسموح به للمنظمه . وبما ان اي منظمه تكون في الاصل عباره عن عدد من الاجهزه الموصله فيما بينها بشبكات داخليه..يجب علينا اذا تحقيق أمن لهذه الشبكات ومنع اختراقها من الخارج وعمل التحديثات الضروريه لتحميل الرقع اللازمه للأجهزه ,ولا ننسى اهميه وجود الصيانه على هذه الشبكات والاجهزه الموجوده.ونصل اخيرا الى وجود نظام يتحكم بهذه الانظمه المتعدده في المنظمه في ظل وجود الاداره الجيده التي تحسن استخدام المزايا والمعلومات المتوافره لدينا ويتظمن ذلك اجراءات كلمات السر المطلوبه وكيفيه ادارتها وفي النهايه يلزم وجود الاشراف المستمر ليدعم هذه الاجراءات ويتأكد من تحقيقها بشكل فعال.

١. ماهي أساسيات أمن المعلومات؟

أساسيات أمن المعلومات هي عباره عن مجموعه من اجراءات أساسيه مشتركه فيما بينها والتي تسعى الى تحقيق أمن معلومات فعلي للمنظمه.ومن هذه الاجراءات مايمكن ايجازه في عده نقاط مع الشرح اللازم:

اولا: تحديد المجال والهدف.
يتعلق بترابط النشاطات المختلفه في المنظمه ببعضها البعض وتحديد مدى المعلومات السموح بها والاجراءات التي من خلالها يتم التعامل مع الموظفين وكذلك مع الاشخاص من خارج المنظمه.اما بما يتعلق بتحديد الهدف فذلك يتم من خلال معرفه الاخطار التي تواجه المنظمه وكيفيه السيطره عليها وماهو المقياس المرجو للأمن في هذه المنظمه.

ثانيا: عمليه الاختيار.
يقصد بهذه العمليه اختيار الاجراءات اللازم توفرها او اللازم عملها اولا في اساسات المنظمه والتي يمكن الاختيار فيما بينها بحسب الاولويه الهامه لكل اجراء.

ثالثا: المواضيع ذات العلاقه بأساسيات أمن المعلومات.
يقصد بذلك التطبيقات ذات العلاقه المباشره بأمن المعلومات في اي منظمه والتي يمكن من خلاله الوصول الى المستوى الأمني المنشود. ومن هذه التطبيقات:

- ماهي الاجراءات التقنيه والاجراءات التنظيميه التي يقبل بها في المنظمه.
- ماهو حد الاخطار والضعف التي يمكن القبول به في داخل المنظمه.
- ماهو الحد الاعلى او الميزانيه المعطاه لتأسيس أمن المعلومات وعلاقتها بما يود عمله.بحيث هل تكون كافيه واخذه جميع الجوانب بعين الاعتبار..وبعد ذلك ننظر الى ماتم تحقيقه فعليا في المنظمه.

واخيرا لاننسى ان بعض الاجراءات يمكن تغييرها او الاضافه عليها او حذفها اثناء العمل وبذلك يجب ان تكون بالمرونه المرجو منها.

٢. سياسات أمن المعلومات.

يقصد بهذه السياسات ان تكون لدى المنظمه تشريعات خاصه بأمن المعلومات اي ان يعرف كل فرد الاجراءات ويسعى الى تطبيقها على المستوى الادنى.
والهدف من سيسات أمن المعلومات الوصول الى الاجراءات التي يلزم كل فرد بأتباعها وتساعد هذه الاجراءات في بناء البنيه التحتيه للمنظمه.ومن هذه السياسات تحديد الوصول المسموح به لكل فرد سواء من داخل او خارج المظمه ومن هذه الاجراءات:

- وجود وثيقه سياسات أمنيه للمنظمه. بحيث يكون هناك عدد من الاجراءات المثاليه المتعارف عليها التي يلزمة اتباعها وعدم تجاوزها.
- تنفيذ هذه السياسات. يكون هناك عدد من الاجراءات التي تتأكد من ان السياسات قد نفذت بالشكل المطلوب.
- تطوير هذه السياسات. ان يكون هناك تطوير لهذه السياسات عند وجود تقنيات جديده او عند سن قوانين في داخل المنظمه.

اذا رأينا انه عند بناء بنيه تحتيه لأمن المعلومات يلزم وجود اولا عدد من السياسات الصارمه التي تضمن الوصول الدرجه الأمنيه المطموح بها.

٣. أمن المنظمه.

يقصد به اداره لأداره أمن المعلومات. ومن ذلك وجود بنيه تحتيه لأمن المعلومات في المنظمه ووجود منظمه أمنيه في داخل المنظمه تضمن تنفيذ الخطط التنفيذيه للأمن ووجود اتصالات وتفاعلات بين اطراف وجهات المنظمه داخليا وتتفاعل هذه الجهات مع البيئه الخارجيه ككتله واحده,ووجود وظيفه اشرافيه تدقق سير العمل واذا لزم الامر تسطيع المنظمه الاستعانه بأستشاري خارجي يقدم نصائح اختصاصيه في أمن المعلومات ويمكن للمنظمه ان تتعاون مع المنظمات الاخرى مستفيده بذلك من الخبرات وبذلك يكون هناك حقل خبرات مشترك بين المنظمات, ولاننسى اهميه وجود سلطه لتقييم الوضع الأمني في المنظمه ويكون افراد هذه السلطه مجموعه يتم اختيارهم من موظفين المنظمه بحيث تقوم بشكل دوري على دراسه وتقييم الأمن المعلوماتي في المنظمه.

٤. المتطلبات الأمنيه الخاصه بالموظفين.

والهدف منها تقليل الاخطاء الأمنيه البشريه او الاحتيال او سوء استعمال السلطات والمعلومات, فالبشر هم من لديهم المعلومات السريه وهم ايضا من يسعى الى اختراق ومعرفه هذه المعلومات. ومن هذه المتطلبات مايمكن ايجازه في النقاط التاليه:

- تعيين الموظفين بشرط تحقق الاداء اللازم للخطط الأمنيه, بحيث ان كل شخص جديد في المنظمه يلزم ان يوافق ويقر بالانظمه الأساسيه الموجوده والتالف معها, ويتطلب ايضا للمواقع الحساسه ان يتم تعيين اشخاص تنطبق عليهم شروط معينه ويخضعوا لاختبارات سابقه بما يضمن قدرتهم على تحمل المسؤوليه والسلامه من تسريب المعلومات, وانه لكل وظيفه وكل منصب له شروط أمنيه مختلفه تعتمد على كميه المعلومات الحساسه المتعامل معها.ولاننسى زوار المنظمه سواء من استشاريين او متدربين لديها يجب ان يتقيدوا بالتعليمات الخاصه بأمن المعلومات.

- التدريب. ويقصد به تدريب الموظفين في المنظمه على كيفيه استخدام برامج أمن المعلومات ويتضمن ذلك انشطه مختلفه تكون كفيله باعطاء الموظف الكميه الكافيه من أمن المعلومات.

- ردود الفعل تجاه التهديدات المحتمله او حوادث الاختراق. من ذلك ان يذكر مثلا حادثه تم بها الحصول على معلومات من المنظمه بطريقه غير شرعيه, لكي يتم تفادي وقوعها مستقبلا.او ذكر تهديد تمت السيطره عليه لكي يكون الموظفين بألمام بمثل هذه التهديدات ان واجهتهم في المستقبل.

- ذكر نقاط الضعف في النظام الأمني للمنظمه. بحيث يلزم الموظفين بأبلاغ رؤسائهم عنها لكي يتم معالجتها في اسرع وقت.

- ذكر نقاط ضعف البرامج لكي يتم تم تطويرها والمساعده من قبل المختصين في المنظمه بذلك.

- اعلان عن الاجراءات التأديبيه التي صدرت في حق الموظفين المخلين بالانظمه الأمنيه داخل المنظمه يكون كفيلا ورادعا لغيرهم.

٥. كيف نحقق بيئه أمن مناسبه؟

يتم ذلك من خلال منع الوصول الغير مسموح به الى المنظمه, ونحاول في المنظمه الى تقسيم الخطط الأمنيه على كل قسم بحيث يمكن السيطره على كل قسم بسهوله وتعيين مسؤولا أمنيا في هذا القسم. من الملاحظ ايضا ان لا ننسى الدخول الفعلي للمنظمه واخذ المعلومات كأن يتم انتحال شخصيه موظفي الصيانه وبذلك يتمكن من الدخول واخذ المعلومات اللازمه.ويجب وجود أمن على مداخل ومخارج مبنى المنظمه ووضع نظم أمنيه مشدده واجهزه مراقبه اللازمه لمنع محاوله الدخول الفعلي الغير شرعي. يلزم ايضا وجود توثيق لعمليات الدخول والخروج.وللحفاظ علي هذه الاجهزه من الحوادث لاسمح الله يلزم وجود نظام انذار مبكر بحدوث حريق مثلا والتدابير اللازمه عند وقوع ذلك كوجود طفايات حريق وقطع التيار الكهربائي ولتفادي كل ذلك يقوم موظفين بعمل الصيانه الدوريه اللازمه للاجهزه والخادمات.

٦.أساسيات أمن الاجهزه والشبكات.

الهدف منها تحقيق أمن وسلامه للاجهزه والشبكات المترابطه بينها في موقع العمل ويكون ذلك بعدد من الاجراءات منها التخطيط السليم للشبكات منها وجود شبكه خاصه بكل قسم بحيث لو تم اختراقها لايتمكن من الدخول الاجهزه الاخرى. وضع اجهزه منع الفيروسات عند المنافذ الخارجيه و يوجد عدد من الاجراءات المتفرقه التي يرجى منها تحقيق السلامه اللازمه ومنها:

- تصميم تدابير أمنيه مشدده للحيال دون الوصول الى الشبكه.
- اداره التطبيق والتي من مهامها التأكيد على تطبيق التطبيقات الأمنيه المختلفه.
- اداره التقنيه والتي تقوم بحل المشاكل التقنيه التي يمكن مواجهتها اثناء العمل.
- اداره التفويض والتوثيق.وهي التي تقوم بتوثيق العمليات الحاصله واعطاء الصلاحيات اللازمه لكل موظف في الحدود المسموحه له.
- مراقبه الاستعمال الصحيح للشبكه والاجهزه .
- وجود حمايه خاصه من الفيروسات وذلك باستخدام الجدار الناري أو استخدام البرامج المضاده والكاشفه للفيروسات.
- منع الرسائل الدعائيه من الدخول الى البريد الاكتروني الخاص بالمنظمه. وبذلك نكون قللنا من التهديدات على المنظمه.
- توفر الرقع اللازم تحميلها على الاجهزه بحيث تقلل من العيوب الأمنيه في النظام.

ويمكن ان نتطرق هنا الى قبول البرامج الجديده بحيث انها تخضع الى اختبارات وقياسات أمنيه للتحقق من امكانيه الوثوق بها و لكي نحافظ على المعلومات لدينا حتى ولو فقدت يلزمنا عمل نسخ احتياطيه للبرمج والمعلومات الهامه لدينا للحيال دون فقدانها ويتطلب ذلك وجو اداره او اشخاص مكلفين من قبلها بعمل نسخ احتياطيه دوريه .
على ايه حال فأن الشبكات والاجهزه هي عباره عن هاردوير اي يلزم عمل صيانه لهم .ويدخل من ضمن أمن الشبكات أمن البريد الاكتروني بحيث تكون هناك شفرات معينه بين المنظمه والمنظمات الاخرى المتعامل معها.

٧.تحقيق أمن فعلي للانظمه في المنظمه.

ويهدف منه اداره السريه الانظمه المختلفه في المنظمه ومن ذلك اداره الحسابات و المسؤوليات وتسجيل المستخدمين وعمل كلمات المرور الخاصه بهم ووجوب المحافظه على هذه الكلمات لضملن أمن معلوماتي جيد وتحديد فتره صلاحيه لها لكي يتم تغيرها بشكل دوري وكما نقول دائما فأنه يلزم وجود مراقبه دائمه على الانظمه والشبكات والموظفين المستخدمين لها .

أخيرا..

ندرك بعد ذلك اهميه أمن المعلومات للمنظمه واهميه بناء بنيه أساسيه قويه لها تضمن هذا الامان..ونلاحظ ايضا انه يمس جميع اطراف المنظمه وبذلك يلزم ان يكون كل فرد فيها ملم بأمن المعومات ولو معلومات سطحيه تضمن لنا عدم تسريب المعلومات..

٨.المراجع:

1. http://enterprisesecurity.symantec.com/content/displaypdf.cfm?ssspdfid=2&EID=0
2. http://www.isaca.org/Content/NavigationMenu/Restricted/Information_Security_Survival_Kit/COBIT_security_baseline_nystate.pdf
3. http://csrc.nist.gov/ispab/2002-06/Rau-06-2002.pdf
4. http://campus.tudelft.nl/live/pagina.jsp?id=63b5e98d-aa80-4199-8947-e89d8d9789d1&lang=en
5. http://www.insecure.org/