أمن المعلومات والبيانات

إعداد الطالب/ محمد علي ابكر علي

أمن المعلومات والبيانات

أمن المعلومات يقصد به تأمين البيانات المتداولة عبر شبكة الانترنت. فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لاخر أصبح النظر إلى أمن تلك البيانات والمعلومات بشكل مهم للغاية. يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات ..

إن حماية المعلومات هو أمر قديم ولكن بدأ استخدامه بشكل فعلي منذ بدايات التطور التكنولوجيا ويرتكز أمن المعلومات إلى:-

- أنظمة حماية نظم التشغيل
- أنظمة حماية البرامج والتطبيقات.
- أنظمة حماية قواعد البيانات.
- أنظمة حماية الولوج أو الدخول إلى الأنظمة.

المبادئ الأساسية

من أهم المفاهيم, ومنذ أكثر من عشرين عاما، وأمن المعلومات قد حددت بالسرية Confidentiality والتكامل Integrity والتوافر Availability(المعروفة باسم الثالوث (سي آي ايه)(CIA),(أعضاء InfoSec التقليديون الثالوث -السرية والتكامل والتوافر - ويشار إليها بالتبادل في الأدبيات على أنها, سمات أمان، خصائص وأهداف أمنية, جوانب أساسية، معايير معلومات، خصائص معلومات هامة, واللبنات الأساسية.) والمبادئ الأساسية لأمن المعلومات. العديد من المتخصصين في مجال أمن المعلومات يؤمنون إيمانا راسخا بأن المساءلة ينبغي أن تضاف كمبدأ أساسي لأمن المعلومات.

في عام 2002، اقترح دون باركر نموذجا بديلا للثالوث التقليدي (CIA). يتكون نموذج باركر من ستة عناصر من أمن المعلومات. العناصر هي السرية، الحيازة، السلامة، الأصالة، التوفر والأداة. إن سداسي باركر هو موضع نقاش بين المتخصصين في مجال الأمن.

أبسط أنواع الحماية هي استخدام نظام التعريف بشخص المستخدم, وثوقية الاستخدام, ومشروعيته. هذه الوسائل تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بالاستخدام. وتضم هذه الطائفة:

كلمات السر بأنواعها.

البطاقات الذكية المستخدمة للتعريف.

وسائل التعريف البيولوجية والتي تعتمد على سمات الشخص المستخدم المتصلة ببنائه البيولوجي.

المفاتيح المشفرة ويمكن ان تشمل ما يعرف بالاقفال الإلكترونية التي تحدد مناطق النفاذ.

إن كل التقنيات التي وصل إليها العالم لا يمكن ان تعيش من دون أمن المعلومات. فعلى سبيل المثال, نظام البنوك لو لم يكن هناك أمن المعلومات لاستطاع أي شخص ان يدخل على النظام ويغير حسابه ويصبح مليونير من لا شيء.

السرية

السرية هو المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالأطلاع عليها أو الكشف عنها. على سبيل المثال، استعمال بطاقة الائتمان في المعاملات التجارية على شبكة يتطلب إدخال رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر لإنجاز وتجهيز المعاملات على الشبكة. يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الإرسال، وذلك بالحد من الوصول إلى أماكن تخزين أو ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، النسخ الاحتياطي، والإيصالات المطبوعة)، وذلك بتقييد الوصول إلى الأماكن التي يتم تخزين الرقم والبيانات بها. اماإذا كان الطرف غير المصرح له قد حصل على رقم البطاقة بأي شكل من الأشكال فإن ذلك يعد انتهاكا لمبدأ السرية في حفظ وتخزين البيانات.

خرق السرية يتخذ أشكالا عديدة. تجسس شخص ما على شاشة الحاسوب لسرقة كلمات سر الدخول ،أو رؤية بيانات سرية بدون علم مالكها, يمكن أن يكون خرقا للسرية. إذا كان الحاسوب المحمول يحتوي على معلومات حساسة عن موظفي الشركة, فإن سرقته أو بيعه يمكن أن يسفر عن انتهاك لمبدأ السرية. إعطاء معلومات سرية عبر اتصال هاتفي هو انتهاك لمبدأ السرية إذا كان طالب الاتصال غير مخول بأن يحصل على المعلومات.

السرية أمر ضروري (لكنها غير كافية) للحفاظ على خصوصية الناس الذين تحتوي الأنظمة معلوماتهم الشخصية.

التكامل (السلامة)

في مجال أمن المعلومات، التكامل (السلامة) يعني الحفاظ على البيانات من التغيير أوالتعديل من الأشخاص غير المخولين بالوصول اليها. عندما يقوم شخص, بقصد أو بغير قصد, بحذف أو انتهاك سلامة ملفات البيانات الهامة أو الإضرار بها, وهو غير مخول بذلك, يعد هذا انتهاكا لسلامة البيانات. وعندما يصيب فيروس حاسوبا, ويقوم بتعديل بياناته أو يتلفها يعد هذا انتهاكا لسلامة البيانات، وكذلك عندما يكون الموظف (غير المخول) قادرا على تعديل راتبه في قاعدة

البيانات والمرتبات، وعندما يقوم مستخدم (غير مصرح له) بتخريب موقع على شبكة الإنترنت، وهلم جرا. و تعني سلامة البيانات كذلك، أن تكون التغيرات في البيانات مطردة، فعندما يقوم عميل البنك بسحب أو إيداع، ينبغي أن ينعكس ذلك على رصيده في البنك.

إن الإخلال بسلامة البيانات ليس بالضرورة نتيجة عمل تخريبي، فمثلاً, الانقطاع في النظام قد ينشئ عنه تغيرات غير مقصودةأو لا تحفظ تغيرات قد تمت فعلاً.

توفر البيانات

يهدف أي نظام للمعلومات لخدمة غرضه، أن تكون المعلومات متوفرة عند الحاجة إليها. وهذا يعني أن تعمل عناصر النظام الآتية بشكل صحيح و مستمر:

الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات.

الضوابط الأمنية المستخدمة لحمايتة النظام.

قنوات الاتصال المستخدمة للوصول.

نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات.

منع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة، اونظام الترقيات والتحديث.

ضمان منع هجمات الحرمان من الخدمة.

إدارة المخاطر

والمعالجة الشاملة لموضوع إدارة المخاطر هو خارج عن نطاق هذا المقال. ومع ذلك، سوف تقدم تعريفا مفيدا لإدارة المخاطر تكون كذلك بعض المصطلحات الأساسية ويشيع استخدامه في عملية إدارة المخاطر.

ينص التعريف التالي لإدارة المخاطر : "إدارة المخاطر هي عملية التعرف على نقاط الضعف والتهديدات الموجهة إلى موارد المعلومات التي تستخدمها المنظمة أو الشبكة المعلوماتية في تحقيق الأهداف التجارية أو الاخرى، والحد والتقليل من نقاط الضعف إن وجدت، لتأخذ في الحد من المخاطر إلى مستوى مقبول، على أساس قيمة موارد المعلومات إلى المنظمة. "

هناك أمران في هذا التعريف قد يحتاجان إلى بعض التوضيح. أولا، عملية إدارة المخاطر هي تكرار العمليات الجارية ويجب أن يتكرر إلى ما لا نهاية لان بيئة العمل المتغيرة باستمرار، والتهديدات الجديدة والضعف تظهر كل يوم. والثانية اختيار التدابير المضادة (الرقابة) المستخدمة لإدارة المخاطر يجب أن توازن بين الإنتاجية، والتكلفة، وفعالية التدابير المضادة، وقيمة الموجودات وحماية البيانات.

الخطر هو احتمال أن شيئا ما سيئا سيحدث يسبب الأذى لأحد الأصول المعلوماتية (أو الخسارة في الأصول). الضعف هو الضعف الذي يمكن أن يستخدم لتعريضها للخطر أو التسبب في ضرر لأحد الأصول المعلوماتية. التهديد أي شيء فعل (من صنع الإنسان او فعل من أفعال الطبيعة) لديه القدرة على التسبب في ضرر.

احتمال أن يشكل تهديدا سوف تستخدم من التعرض للضرر يتسبب في خطر. عندما لا يشكل تهديدا استخدام الضعف لإلحاق الاذى، لما له من أثر. في سياق أمن المعلومات، وأثر هو خسارة لتوافر والنزاهة والسرية، وربما غيرها من الخسائر (الدخل المفقود، والخسائر في الأرواح وخسائر في الممتلكات العقارية). وتجدر الإشارة إلى أنه ليس من الممكن تحديد جميع المخاطر، ولا هو ممكن القضاء على جميع المخاطر. المخاطر المتبقية تسمى المخاطر المتبقيه.