محاضرة: امن المعلومات

تمهيد

مع تطور أساليب الاختراق والقرصنة ومع زيادة الاعتماد على قواعد البيانات المرتبطة بالانترنت، أصبحت حماية قواعد البيانات بالإضافة الى نظام المعلومات عامة من التحديات التي تواجهها المؤسسات المختلفة لا سيما مع تزايد احداث وجرائم السرقات الالكترونية.

مفهوم امن المعلومات

أمن المعلومات يعني إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص اخر دون اذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول الى معلوماتك الخاصة، كما يعني امن المعلومة منع وصول الافراد الغير مصرح لهم منع تعديل البيانات، منع أخذ المعلومات، حماية المصادر وذلك بعرقلة الهجمات.

عناصر أمن المعلومات

من اجل حماية المعلومات من المخاطر التي تتعرض لها لا بد من توفر مجموعة من العناصر التي يجب اخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد صنف تلك العناصر الى 5 وهي:

1. **السرية او الموثوقية:** وهي تعني التأكد من ان المعلومات لا يمكن الاطلاع عليها او كشفها من قبل أشخاص غير مصرح لهم بذلك ولتجسيد هذا الامر يجب على المؤسسة استخدام طرق الحماية المناسبة من خلال استخدام وسائل عديدة مثل عمليات تشفير الرسائل او منع التعرف على حجم تلك المعلومات أو مسار إرسالها.
2. **التعرف او التحقق من الهوية الشخصية:** وهذا يعني التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما اذا كان هو المستخدم الصحيح لتلك المعلومات ام لا، ويتم ذلك من خلال استخدام كلمات السر الخاصة بكل مستخدم.
3. **سلامة المحتوى:** وهي تعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله او تدميره او العبث به في أي مرحلة من مراحل المعالجة او التبادل سواء كان التعامل داخليا في المشروع او خارجيا من قبل أشخاص غير مصرح لهم بذلك ويتم ذلك غالبا بسبب الاختراقات الغير مشروعة مثل الفيروسات حيث لا يمكن لأحد أن يكسر قاعدة بيانات البنك ويقوم بتغيير رصيد حسابه لذلك يقع على عاتق

المؤسسة تأمين سلامة المحتوى من خلال اتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات او الفيروسات.

4. **استمرارية توفير المعلومات او الخدمة:** وهي تعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمات لمواقع المعلومات وضمان عدم تعرض مستخدمي تلك المعلومات الى منع استخدامها او الوصول اليها بطرق غير مشروعة يقوم بها اشخاص لإيقاف الخدمة بواسطة كم هائل من الرسائل العبثية عبر الشبكة الى الأجهزة الخاصة لدى المؤسسة.

5. **عدم الإنكار**: ويقصد به ضمان عدم إنكار الشخص الذي قام بإجراء معين متصل بالمعلومات لهذا الاجراء، ولذلك لا بد من توفر طريقة او وسيلة لإثبات أي تصرف يقوم به أي شخص للشخص الذي قام به في وقت معين، ومثال ذلك للتأكد من وصول بضاعة تم شراؤها عبر شبكة الانترنت الى صاحبها، ولإثبات تحويل المبالغ الكترونيا يتم استخدام عدة رسائل مثل التوقيع الالكتروني والمصادقة الالكترونية.

- **الهدف من تهديد المعلومات:**
- تدمير واتلاف الأجهزة والمعلومات.
- سرقة او تعديل المعلومات.
- وضع أنظمة للتجسس والمراقبة.
- **أنواع المشاكل الأمنية:**

تحدث المشكلة الأمنية عندما يتم اختراق النظام المعلوماتي من خلال احد المهاجمين او المتسللين "الهاكر" او الفيروسات او نوع اخر من أنواع البرامج الخبيثة.

أ. **الهاكر:** هو الشخص يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي، وقد اصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة.

ب. **البرمجيات الخبيثة:** وهي عبارة عن برامج تم إعدادها من قبل مبرمجين وذلك لغرض إلحاق الضرر بالبيانات المستهدفة كتخريبها وإزالتها او السيطرة عليها وإلحاق الضرر بها. وتتميز هذه البرامج بقدرتها على التناسخ والانتشار والانتقال من مكان لاخر.

ت. **اختراق:** يعرف الاختراق بالقدرة الى الوصول الى اهداف معينة بطريقة غير مشروعة، وذلك عن طريق الثغرات الموجودة في أنظمة تلك الأهداف، وتتنوع دوافع المخترقين فمنهم من يتخذ الاختراق لدافع سياسي وعسكري أو لدافع شخصي او لدافع تجاري.....الخ.

ث. **التجسس:** وهو أسلوب يشبه في حد ذاته الاختراق إلا أن الغرض منه معرفة محتويات الأنظمة المستهدفة دون الإضرار بها، وغالبا ما تتم عن طريق نوع من الفيروسات الذي يقوم بإرسال نسخ من المعلومات والبيانات او التمكين من الدخول الى الأنظمة ومعرفة محتوياتها.

سياسة الحماية:

- يمكن حماية أنظمة المعلومات من خلال اتباع الطرق التالية:

✓ مسح كلمة السر الخاصة بالموظف المنتهي عقده فورا مع المؤسسة.

✓ وضع حساسات مياه او حرائق قرب أجهزة تخزين البيانات.

✓ استخدام الجهاز الخاص بالمؤسسة للأنترنت ويمنع استخدام جهاز غيره مثلا منع إحضار الموظف لجهازه الخاص به.

✓ تحديد صلاحيات كل مستخدم على البيانات الموجودة على قاعدة البيانات.

✓ الدخول للمؤسسة عن طريق بطاقة خاصة.

✓ وضع مثلا أجهزة التحقق من بصمة الشخص على أجهزة البيانات المهمة.

✓ التأمين المادي للأجهزة والمعدات.

✓ تركيب مضاد فيروسات قوي في فترات قصيرة.

✓ تركيب أنظمة كشف الاختراق وتحديثها.

✓ تركيب أنظمة مراقبة الشبكة للتنبيه عن نضاط الضعف التأمينية.

✓ استخدام أنظمة قوية لتشفير المعلومات المرسلة.

✓ استخدام الأجهزة البيولوجية كفحص بصمة الاصبع او شبكة العين.

✓ سياسة تواجد اكثر من شخص في غرفة الخادم وخاصة عند عمل شخص مباشرة على الخادم.

✓ سياسة تفتيش الموظفين عند المغادرة من المؤسسة.

✓ دراسة ومواكبة أساليب حيل الاختراق.

✓ الدراسة والفهم الجيد لنظم تشغيل وإدارة الشبكات.

✓ عمل سياسات التأمين ومراجعتها كل فترة.