أمن المعلومات الالكترونية

مقدّمة

إنّ التقدم التكنولوجي الكبير، وتطوّر وسائل التواصل والاتصال المتنوعة، وانفتاح العالم على بعضه، واعتماده على إرسال شتى أنواع البيانات خلال الشبكات، كلّ ذلك أدى إلى إحداث خطر على تسرّب هذه البيانات، ووصولها للأشخاص الخاطئين، أو المنافسين، وبالتّالي أصبحت الحاجة الملحّة للحفاظ على أمن المعلومات.

أمن المعلومات

أمن المعلومات هو السيطرة التّأمة على المعلومات، من حيث تحديد من سيستلم هذه البيانات، وتحديد صلاحيّات الوصول إليها، واستخدام مجموعة من التقنيّات من أجل ضمان عدم اختراقها من قبل أي جهة، وتتضاعف أهميّتها من الحفاظ على الخصوصيّة، إلى الحفاظ على بيانات هامّة مثل حسابات العملاء في البنوك.

مخاطر الإنترنت على أمن المعلومات

يوجد في شبكة الإنترنت الاعتيادية مجموعة كبيرة من نقاط الضعف التي تمكّن أشخاص غير مخوّلين من الوصول إلى هذه البيانات، ومنها الأخطاء البرمجيّة التي يقوم بها المبرمجون أثناء بناء الشبكات، أو تصميم التطبيقات المختلفة، مثل أخطاء في كيفيّة تعامل التطبيق مع الإدخال الخاطئ، أو بسبب سوء توزيع الذاكرة، كما أنّ هناك العديد من المبرمجين الذين يقومون بتصميم برامج مخصّصة لاختراق الأنظمة، والبحث عن نقاط ضعفها.

طرق المحافظة على أمن المعلومات

يتمّ اللجوء لمجموعة من طرق الحماية من أجل الحفاظ على أمن المعلومات، ومنها:

- طرق الحماية الماديّة: هناك العديد من الطرق البسيطة التي يجب اتّباعها من أجل الحفاظ على أمن المعلومات، وهو الحفاظ على جهاز الحاسوب في مكان آمن، ووضع كلمة سرّ عليه لمنع عبث المتطفلين، وأن تكون كلمة السر تحتوي على أحرف، وأرقام، ورموز؛ كي يصعب التنبّؤ بها، وتغييرها بشكل دوري.
- استخدام الجدار الناري (Firewall) :الجدار الناري هو عبارة عن جهاز، أو تطبيق، ويتمّ وضعه عند الخادم، وعند مصافي الشبكة، كلٌ حسب احتياجاته.
- التشفير: هناك العديد من البروتوكولات المعدة لتشفير البيانات، بحيث تمنع أي أحد يصل لها او فهمها، وتختلف درجة التعقيدات في هذا التشفير، فهناك بعض الأنظمة التي يمكن حلها بالعودة لقواعد تشفيرها، ولذلك يجب اعتماد طريقة معقدة، تصعّب قدر الإمكان إمكانيّة إعادة النص للغته قبل التشفير، وبالطبع فإنّ مفتاح فكّ التشفير يمتلكه الجهاز المستقبل لهذه البيانات.
- مراقبة البيانات :(Packet Sniffers) يوجد العديد من التطبيقات التي تمكن من معرفة حركة البيانات الخارجة، والداخلة إلى الشبكة، وعن طريق تحليلها يمكن التوصل للاختراقات التي حدثت لهذه الشبكة، ومعرفة مكانها. كلّما زادت أهميّة البيانات وسريتها، زادت الوسائل المتبعة لحمايتها، من ماديّة، وبرمجيّة، فمثلاً أجهزة

الخوادم توضع في مكان محمي بشتّى الطرق الفيزيائيّة، ومن ضمنها الحراس.