**أمن وسرية المعلومات**

**security and secret of information**

**مقدمة**

يعد التطور السريع في تكنولوجيا المعلومات والإنتشار الواسع للنظم والبرامج وتطور ووسائل تخزين االمعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لأخر أدى إلى أن تكون هذه المعلومات عرضة للإختراق لذلك أصبحت هذه التقنية سلاحا ذو حدين تحرص المنظمات على إقتناءه و توفير سبل الحماية له ، إن موضوع الأمن المعلوماتي يرتبط ارتباطا وثيقاً بأمن الحاسوب فلا يوجد أمن للمعلومات إذا لم يراعى أمن الحاسوب ، وفي ظل التطورات المتسارعة في العالم والتي أثرت على الإمكانات التقنية المتقدمة المتاحة والرامية إلى خرق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب ، وتجدر الإشارة إلى أن أعمال التجارية على شبكة الانترنت والتي تتطلب الملايین من التبادلات المصرفیة السرية أصبحت قريبة من متناول الكثیرين كان لابد من التفكير الجدي لتحديد الإجراءات الدفاعية والوقائية وحسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب ، ومن هنا تظهر مهمة جديدة ومسؤولية كبيرة أمام إدارة نظم المعلومات في المنشأة وهي ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل هذه النظم بشكل صحيح والتخطيط الدقيق لمواجهة جميع الأخطار التي يمكن أن تؤدي إلى تعطلها أو توقفها عن العمل، وفي حال حدوث ذلك، التمكن من إعادة تشغيلها بأسرع وقت ممكن، وتسمى هذه الوظيفة الهامة والضرورية جدا حماية وأمن نظم المعلومات، وتهدف هذه الوظيفة إلى حماية الموارد المحوسبة من الأخطار والتهديدات المقصودة وغير المقصودة التي يمكن أن تؤدي إلى عمليات غير مسموح بها مثل تعديل أو انكشاف أو تخريب البيانات أو البرامج.

**مفهوم أمن المعلومات Information Security**

**يعرف امن المعلومات بأنه(**(أمن المعلومات هو حماية ووقاية للمعلومات من الإخطار الداخلية، والخارجية والمتمثلة بالسرقة والتزوير والتلاعب بالمعلومات بشكل متعمد )) **ويعرف** [**أمن**](http://ar.wikipedia.org/wiki/%D8%A3%D9%85%D9%86) **المعلومات** بأنه ((العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة و البرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال.

**الوسائل الأساسية لنظام الأمن المعلوماتي في منظمات الإعمال**

إن النظام الأمني الفعال يجب أن يشمل جميع الوسائل ذات الصلة بنظام المعلومات المحوسبة ويمكن تحديد هذه الوسائل بما يلي :

1. **منظومة الأجهزة الإلكترونية و ملحقاتها :**

إن أجهزة الحواسيب تتطور بشكل جداً بالمقابل هناك تتطور في مجال السبل المستخدمة لإختراقها مما يتطلب تطوير القابليات و المهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب و العبث المقصود في الأجهزة أو غير المقصود .

1. **الأفراد العاملين في أقسام المعلومات :**

يلعب الفرد دورا أساسيا ومهما في مجال أمن المعلومات والحواسيب و له تأثير فعال في أداء عمل الحواسيب بجانبيه الإيجابي و السلبي ، فهو عامل مؤثر في حماية الحواسيب و المعلومات و لكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة وسرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير ، إن من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين و وضع تعليمات واضحة لاختيارهم وذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد .

1. **البرمجيات المستخدمة في تشغيل النظام :**

تعتبر البرمجيات من المكونات غير المادية وعنصر أساس في نجاح استخدام النظام ، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية و يمكن أن تحقق حماية للبرامج وطرق حفظ كلمات السر وطريقة إدارة نظام التشغيل وأنظمة الإتصالات ، إن أمن البرمجيات يتطلب أن يؤخذ هذا الأمر بعين الإعتبار عند تصميم النظام و كتابة برامجه من خلال وضع عدد من الإجراءات كالمفاتيح و العوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها و تمنع أي شخص من إمكانية التلاعب والدخول إلى النظام و ذلك من خلال أيضا تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها ،و محاولة التمييز بين اللذين يحق لهم الإطلاع وحسب كلمات السر الموضوعة .

1. **شبكة تناقل المعلومات :**

تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الإتصالات كما أنها سهلت عملية التراسل بين الحواسيب و تبادل و استخدام الملفات ، و لكن من جهة أخرى إتاحة عملية سرقة المعلومات أو تدميرها سواء من الداخل كإستخدام الفيروسات أو من خلال الدخول عبر منظومات الاتصال المختلفة ،لذلك لا بد من وضع إجراءات حماية و ضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات و توفير الأجهزة الخاصة بالفحص ، كما أن نظم التشغيل المستخدمة والمسؤولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة و قدرة عالية على الكشف عن التسلل إلى الشبكة و ذلك من خلال تصميم نظم محمية.

1. **مواقع( الأبنية) منظومة الأجهزة الإلكترونية و ملحقاتها :**

يجب أن تعطى أهمية للمواقع والأبنية التي يحوي أجهزة الحواسيب وملحقاتها ، وحسب طبيعة المنظومات و التطبيقات المستخدمة يتم إتخاذ الإجراءات الإحترازية لحماية الموقع وتحصينه من أي تخريب والتحقق من هوية الأفراد الداخلين و الخارجين من الموقع و عمل سجل لذلك .

**الأخطار التي يمكن أن تتعرض لها أنظمة المعلومات المعتمدة على الحاسب**

تعتبر المخاطر المقصودة أشد خطرا على أداء فعالية النظم وتزداد تلك الخطورة في النظم الإلكترونية، وتكمن خطورة مشاكل أمن المعلومات في عدة جوانب منها تقليل أداء الأنظمة الحاسوبية، أو تخريبها بالكامل مما يؤدي إلى تعطيل الخدمات الحيوية للمنشأة، أما الجانب الآخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الاطلاع والتصنت على المعلومات السرية أو تغييرها إلى خسائر مادية أو معنوية كبيرة

**ويمكن تصنيف المخاطر عدة أنواع :**

**أولا/ من حيث مصدرها**

* **مخاطر داخلية**

حيث يعتبر موظفي المنشآت هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات وذلك لأن موظفي المنشآت على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم لهذا النظام ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم، ولذلك فإن موظفي الشركة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تغييرها.

* **مخاطر خارجية**

وتتمثل في أشخاص خارج المنشأة ليس لهم علاقة مباشرة بالمنشأة مثل قراصنة المعلومات والمنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات سرية عن المنشأة والتي قد تحدث تدمير جزئي أو كلي للنظام في المنشاة.

**ثانيا / من حيث المتسبب بها**

* **مخاطر ناتجة عن العنصر البشري**

و هي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو إثناء إدخالها إلى النظام ، أو في عمليات تحديد الصلاحيات للمستخدمين ، و تشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن و سلامة نظم المعلومات في المنظمات .

**متطلبات تحقيق الأمن والسرية للمعلومات**

**Requirements to achieve security and confidentiality for information**

لكي نحقق الأمن والسرية لمعلومات الشركة يجب أن نضع بعض السياسات والإجراءات التي تستوجب لتوفير الحماية الكافية للمعلومات لعدم الاطلاع عليها من قبل الآخرين غير المصرح لهم ، توجد طرائق مهمة لتقليل المخاطر أو الحد منها وهذه الطرائق : -

1. البناء السليم لنظام المعلومات هو البداية الصحيحة لوضع إستراتيجية فاعلة لمراقبة وتقويم النظام ولحماية آمنة وسلامة موارده .
2. تدريب المستخدمين لنظام المعلومات في مجالات أمن المعلومات،أمن قواعد البيانات , وأمن الشبكات .
3. تطبيق إجراءات جدية وحازمة لحماية البرامج والأجهزة منذ اللحظة الأولى لتشغيل نظام المعلومات .
4. استخدام برنامج الحماية الجدران النارية ( fire walls ) للحماية من الاختراق للأجهزة .
5. استخدام برنامج مكافحة الفيروسات (Anti – virus ) للحماية من الفيروسات المختلفة .
6. عمل النسخ الاحتياطي (Back – up ) وهذا يعالج مشكلة فقدان المعلومات .

**عناصر حماية أمن المعلومات من المخاطر**

منأجل حماية المعلومات من المخاطر التي تتعرض لها لا بد من توفر مجموعة من العناصر التي يجب أخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد صنفت تلك العناصر إلى خمسة عناصر وهي:

**1- السرية أو الموثوقية ((Confidentiality**

وهي تعني التأكد من أن المعلومات لا يمكن الاطلاع عليها أو كشفها من قبل أشخاص غير مصرح لهم بذلك ولتجسيد هذا الأمر يجب على المؤسسة استخدام طرق الحماية المناسبة من خلال استخدام وسائل عديدة مثل عمليات تشفير الرسائل أو منع التعرف على حجم تلك المعلومات أو مسار إرسالها .

**2- التعرف أو التحقق من هوية الشخصية (Authentication)**

وهذا يعني التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما إذا كان هو المستخدم الصحيح لتلك المعلومات أم لا، ويتم ذلك من خلال استخدام كلمات السر الخاصة بكل مستخدم.

**3- سلامة المحتوى (Integrity)**

وهي تعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو تدميره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء كان التعامل داخليا في المشروع أو 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 إتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات أو الفيروسات .

**4- استمرارية توفر المعلومات أو الخدمة (Availability)**

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 إلى منع استخدامها أو الوصول إليها بطرق غير مشروعة يقوم بها أشخاص لإيقاف الخدمة بواسطة كم هائل من الرسائل العبثية عبر الشبكة إلى الأجهزة الخاصة لدى المؤسسة .

**طرق حماية امن المعلومات في منظمة الإعمال**

1. **التشفير**  Encryption

**يعرف** ((**التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى)، لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها ))،** ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة ، ومن المعلوم أن الانترنت يشكل في هذه الأيام الوسط الأضخم لنقل المعلومات، ولابد من نقل المعلومات الحساسة (مثل الحركات المالية) بصيغة مشفرة إن أريد الحفاظ على سلامتها وتأمينها من عبث المتطفلين والمخربين واللصوص ،وتستخدم المفاتيح في تشفير الرسالة وفك تشفيرها، وتستند هذه المفاتيح إلى صيغة رياضية معقدة (خوارزميات)

ومن ناحية أخرى فان فك التشفير هو عملية إعادة تحويل البيانات إلى صيغتها الأصلية، وذلك باستخدام المفتاح المناسب لفك التشفير، وسنوضح ذلك في الشكل الآتي لعملية التشفير وفك التشفير.



**النص الأصلي**

**التشفير**

**النص المشفر**

**فك التشفير**

**النص الأصلي**

الشكل يمثل عملية التشفير وفك التشفير

**استخدامات التشفير**

إذا فان الهدف الأساسي للتشفير هو الحفاظ على النص الواضح (أو المفتاح، أو كليهما) بصورة سرية بعيدًا عن الأعداء على افتراض أنهم يملكون كامل القدرة للوصول إلى الاتصالات بين المرسل والمستقبل ، إذن الهدف من عملية التشفير هو ضمان الخصوصية وذلك بالاحتفاظ بالمعلومات بصيغة مخفية على أي شخص آخر، وابرز استخداماته :-

1. الاطلاع على المعلومات المحظورة
2. تأخير إيصال بعض الرسائل وتغير محتويات الرسائل المتبادلة
3. انتحال شخصية المستخدم الحقيقي
4. تغير كلمة السر الخاصة بالمستفيدين
5. **الجدار الناري Fire Wall**

**تعريف** الجدار الناري ((**بأنه مجموعة من الإجراءات المتكاملة والمصممة لمنع الوصول الإلكتروني غير المعتمد إلى شبكة الحاسب** ، ويمكن تعريفه كذلك ((**بأنه عبارة عن مجموعة أنظمة توفر سياسات أمنية بين الإنترنت وشبكة المؤسسة لتجبر جميع عمليات العبور إلى الشبكة والخروج منها أن تمر بالجدار الناري الذي يصد المستخدمين المتطفلين غير المخولين بالدخول إلى أي شبكة خاصة**)) .

فالجدار الناري يكون بمثابة حاجز بين شبكة أي مؤسسة والإنترنت، إذ يعمل كممر يختلف عن أي ممر آخر، وهو ما يوفر سياسات أمنية للمستخدمين، مثل سياسات الشركة التي تحدد الدخول إلى الشبكة والخدمة والتحقق من المستخدم المحلي والخارجي، ونظام الدخول والخروج، وتشفير المعلومات، وإجراءات الحماية من الفيروسات، فالجدار الناري يعمل كجسر إلكتروني يراقب عمليات الدخول والخروج من والى الشبكة وكما موضح في الشكل التالي

