أهمية أمن نظم المعلومات لدى المؤسسات الإقتصادية الحديثة

The Importance Of Securing Information Systems In Modern Economic Enterprises

د. بن الطيب إبراهيم – جامعة الشلف–
benettayeb.ibrahim@gmail.com

ملخص : مع زيادة توجه الإقتصاديات الصناعية نحو الإقتصاديات القائمة على المعلومات حول المنتجات والعملاء والنمو الكبير في استخدام المعاملات الإلكترونية عبر الأنترنت، أدى إلى زيادة الإهتمام بأمن هذه المعلومات، فالمعلومات التنظيمية هي رأس المال الفكري، فكما تحمي المؤسسات أصولها، بحفظ الأموال في البنوك وتوفير بيئة عمل آمنة للموظفين، فعليها أيضا حماية رؤوس أموالها الفكرية.

فرأس المال الفكري للمؤسسة يشمل كل شيء من براءات الإختراع إلى المعاملات والمعلومات التحليلية، ومع الخروقات الأمنية الآخذة في الإرتفاع، وتزايد قراصنة الحاسوب في كل مكان، أجبر المؤسسات على وضع تدابير أمنية قوية من أجل البقاء.

وإن زيادة وانتشار استخدام نظم المعلومات القائمة على أجهزة الحاسوب، أدى ذلك إلى زيادة تهديدات سلامة البيانات وموثوقية المعلومات، ولذلك يجب على المؤسسات التعامل بجدية مع المخاطر والتهديدات الطبيعية والبشرية على حد سواء؛ في الواقع لا توجد وسيلة أمنية شاملة على نظام المعلومات ضد كل حادث محتمل، ولكن هناك طرق للتقليل من المخاطر واسترداد الخسائر.

الكلمات المفتاحية: أنظمة المعلومات، أمن أنظمة المعلومات، الحاسوب، الهجمات الإلكترونية.

تصنيفJEL : D82، D80

Abstract :

As industrial economies move toward information-based economies, their information on products and customers become more valuable, and security becomes more important. Organizational information is intellectual capital. Just as organizations protect their assets keeping their money in an insured bank or providing a safe working environment for employees they must also protect their intellectual capital.

An organization's intellectual capital includes everything from its patents to its transactional and analytical information. With security breaches on the rise and computer hackers everywhere, an organization must put in place strong security measures to survive.

As the use of computer-based information systems has spread, so has the threat to the integrity of data and the reliability of information. Organizations must deal seriously with the risks of both natural and human menaces, Indeed, there is no way to fully secure an information system against every potential mishap, but there are ways to significantly reduce risks and recover losses.

Key words : Information systems, Information systems security, Computer, Cyberattacks..

(JEL) Classification : D80 ،D82

مقدمة:

إن التطورات الحديثة في تقنية المعلومات أحدثت تغيرات مستمرة ومضطردة في أساليب العمل والميادين كافة، إذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية والدولية وأجهزة الحاسوب من الأمور الروتينية في عصرنا الحالي وإحدى علامات العصر المميزة التي لا يمكن الإستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الأعمال وتطوير أساليب خزن وتوفير المعلومات حيث أن انتشار أنظمة المعلومات المحوسبة أدى إلى أن تكون عرضة للإختراق لذلك أصبحت هذه التقنية سلاحا ذو حدين تحرص المؤسسات على إقتناءها وتوفير سبل الحماية لها .

وإن موضوع الأمن المعلوماتي يرتبط ارتباطا وثيقا 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، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية والوقائية وحسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب، وكان على إدارة المؤسسات أن تتحمل مسؤولية ضمان خلق أجواء أمنية للمعلومات والتي تضمن الحفاظ عليها .

وعلى هذا الأساس تأتي أهمية أمن المعلومات والتي سنحاول في هذه الورقة البحثية توضيح جوانب مختلفة لهذه المسألة، ففي البداية سنلقي نظرة عامة حول أمن نظم المعلومات ثم ندرس الأنواع المختلفة من المخاطر التي تتعرض لها أنظمة المعلومات، وفي الأخير نتعرف على كيفية أمن أنظمة المعلومات وحمايتها من الأخطار والطرق والأساليب المتبعة في ذلك، ولهذا نهدف من خلال هذه المقالة تحقيق عدة نقاط، نلخصها في الآتي:

1. شرح ما المقصود بمصطلح "أمن نظم المعلومات"، وما هي الأهداف الرئيسية التي يسعى إليها.
2. تعريف جرائم الحاسوب ووصف العديد من أنواعها، بتبيان المخاطر التي تتعرض لها نظم المعلومات، مع إبراز مصادر وأنواع التهديدات الأمنية.
3. وصف الأنواع المختلفة من التدابير الأمنية التي يمكن تنفيذها لحماية البيانات وأنظمة المعلومات.

1- مفهوم أمن نظم المعلومات والهدف منها:

تشكل المعلومات للمؤسسات البنية التحتية التي تمكنها من أداء مهامها، إذ أن نوع المعلومات وكميتها وطريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل المؤسسات الحديثة، وعليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لإستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، لذا فإن المشكلة التي يجب أخذها بالحسبان هو توفير الحماية اللازمة للمعلومات وإبعادها عن الإستخدام غير المشروع لها .

1/1- تعريف أمن نظم المعلومات:

من أجل فهم أمن نظم المعلومات Securing Information Systems لابد من تحديد معناه، حيث عرفه (السالمي) بأنه مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال، أما (المشهداني) فقد عرفه بأنه الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من مخاطر الضياع والتلف أو من مخاطر الإستخدام غير الصحيح سواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية[1]،

ويشير كل من (Kenneth & Laudon) أن مفهوم أمن المعلومات يتسع ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية (من أجهزة وبرمجيات وبيانات وأفراد) من التجاوزات والتداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل أو كنتيجة لإجراءات خاطئة أو الإستخدام غير الصحيح من إدارة هذه المصادر[2].

أما Effy Oz يعطي التعريف التالي "الأمن يشير إلى السياسات والإجراءات، والتدابير التقنية المستخدمة لمنع الوصول الغير المصرح به، التغيير والسرقة، أو الأضرار المادية لنظم المعلومات[3].

كخلاصة فإن أمن نظم المعلومات من زاوية أكاديمية[4]، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الإعتداء عليها أو استغلال نظمها في ارتكاب الجريمة.

2/1- تطور مفهوم أمن نظم المعلومات:

مفهوم أمن نظم المعلومات مر بمراحل تطورية عدة أدت إلى ظهور ما يسمى بأمن نظم المعلومات، ففي الستينات كانت الحواسيب هي كل ما يشغل العاملين في أقسام المعلومات، وكان همهم هو كيفية تنفيذ البرامج والإيعازات ولم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الأجهزة وكان مفهوم الأمنية يدور حول تحديد الوصول أو الإطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب في الأجهزة لذلك ظهر مصطلح أمن الحواسيب Computer Security والذي يعني حماية الحواسيب وقواعد البيانات، ونتيجة للتوسع في استخدام أجهزة الحاسوب و ما تؤديه من منافع تتعلق بالمعالجة للحجم الكبير من البيانات، تغير الإهتمام ليمثل السيطرة على البيانات وحمايتها.

وفي السبعينات تم الانتقال إلى مفهوم أمن البيانات (Data Security) ورافق ذلك استخدام كلمات السر البسيطة للسيطرة على الوصول للبيانات إضافة إلى وضع إجراءات الحماية لمواقع الحواسيب من الكوارث و اعتماد خطط لخزن نسخ اضافية من البيانات و البرمجيات بعيدا عن موقع الحاسوب، وفي مرحلة الثمانينات والتسعينات ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم للمشاركة في قواعد البيانات، كل هذا أدى الى الإنتقال من مفهوم أمن البيانات إلى أمن المعلومات، وأصبح من الضروري المحافظة على المعلومات وتكاملها وتوفرها ودرجة موثوقيتها، حيث أن الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة وتقلص اختراق المعلومات والتلاعب بها، وكانت شركة IBM الأمريكية أول من وضع تعريف لأمن المعلومات، و كانت تركز على حماية البيانات من حوادث التزوير، والتدمير أو الدخول غير المشروع على قواعد البيانات وأشارت الشركة إلى أن أمناً تام للبيانات لا يمكن تحقيقه ولكن يمكن تحقيق مستوى مناسب من الأمنية.

أما الهدف من وجود نظم المعلومات فكانت نتيجة تطور، وتنفيذ، وصيانة أنظمة المعلومات والتي تشكل جزءا كبيرا ومتزايدا من تكلفة ممارسة نشاط الأعمال، وحماية هذه الموارد هي الشغل الشاغل للمؤسسات اليوم، وإن الإعتماد المتزايد على نظم المعلومات جنبا إلى جنب مع العالم الخارجي من خلال الشبكة العامة، وشبكة الإنترنت يجعل تأمين نظم المعلومات للمؤسسات تحديا متزايدا، ودور رقابة الكمبيوتر والأمن هو لحماية النظم ضد الحوادث العرضية والسرقة والفساد المتعمد للبيانات والتطبيقات، كما أنها تساعد على ضمان أداء المؤسسات لعملياتها

والإمتثال للقانون ومع توقعات الموظفين والعملاء لخصوصية المعلومات، ولهذا فإن الأهداف الرئيسية لأمن نظم المعلومات يمكن تلخيصها كما يلي[5]:

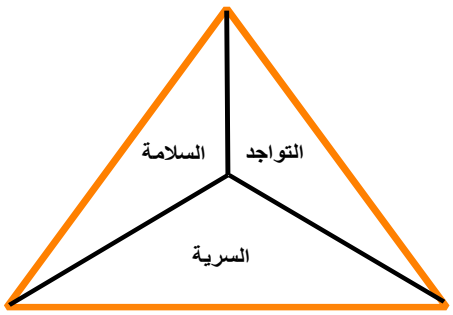
أ. تقليل مخاطر توقف عمل الأنظمة والمؤسسات الإقتصادية.

ب. الحفاظ على سرية المعلومات.

ج. ضمان سلامة وموثوقية مصادر البيانات.

د. ضمان توفر دون انقطاع مصادر البيانات والعمليات عبر الأنترنت.

ه. ضمان الإمتثال للسياسات والقوانين المتعلقة بالأمن والخصوصية.



ولتخطيط التدابير لدعم هذه الأهداف، المؤسسات يجب أن تكون على علم للمخاطر المحتملة لمصادر المعلومات، والتي تشمل الأجهزة والتطبيقات والبيانات والشبكات، ثم عليها تنفيذ التدابير الأمنية للدفاع ضد هذه المخاطر.

أولا/3- عناصر أمن المعلومات:

من المهم توافر عناصر أمن المعلومات في المعلومات المطلوب الحفاظ عليها وعدم كشفها للآخرين، ويختلف مدى أهمية توافر هذه العناصر جميعًا باختلاف أهمية المعلومات محل الحماية واستخداماتها، ويجب التنبيه على أن خرق أو انتهاك أحد هذه العناصر يفقد أمن المعلومات أهميته فهي تعتبر دعائم أساسية لمفهوم أمن المعلومات لدينا ثلاث عناصر أساسية في أمن المعلومات[6] :

الشكل 1-1: عناصر أمن المعلومات

المصدر: آلاء سعد العلي، مرجع سابق، ص:4.

أ- **السرية (الموثوقية):** ويقصد بها حماية المعلومات من أن يطلع عليها أشخاص غير مرخص لهم الوصول إليها وكشفها وربما استخدامها استخداماً سلبياً يضر صاحبها سواء بشكل مباشر أو غير مباشر، لذلك يجب أن نحدد هل المعلومات التي تخصنا تتطلب السرية والخصوصية وإعطاء صلاحيات معينة لأطراف أخرى لـ (قراءتها، تعديلها، التحكم الكامل بها ..)، ويمكن تحديد هذه الصلاحيات من خلال التساؤلات التالية:

- ماهي قيمة هذه المعلومات ؟
- ماذا لو اطلع طرف خارجي عليها ؟ ماهي العواقب المترتبة على ذلك ؟

- هل تستدعي هذه المعلومات اطلاع أطراف أخرى عليها،ومن هم هؤلاء، وما هي حدود صلاحياتهم ؟

فتعتبر السرية أول وأهم عناصر أمن المعلومات والتي ينبغي توخي الحذر وتطبيقها في تعاملاتنا الإلكترونية التي تتطلبها، على سبيل المثال : اعتماد كلمة سر للبريد الإلكتروني قوية وصعبة الإختراق والحرص على عدم كشفها للآخرين وتغييرها من فترة إلى أخرى لضمان السرية.

ب- سلامة المحتوى: ويقصد بها سلامة المعلومات من التغيير أو التعديل عليها أو حذفها من قبل أشخاص غير مرخص لهم بعمل ذلك، ويترتب على انتهاك هذا العنصر عواقب شديدة تبعًا لأهمية المعلومات المستهدفة، كمثال على ذلك : لو اخترق أحدهم جهازك وقام بتغيير البيانات في أحد ملفاتك الخاصة بعملك، قد يكون هذا التغيير من الصعب اكتشافه وبالتالي قد يؤثر على مكانتك وجودة عملك وتتعرض للعقاب من قبل مديرك في العمل، لذلك لابد من التأكد من عمل جميع التحصينات التي تحمي أمن معلوماتك وتضمن العنصر الثاني سلامة المحتوى .

ج-: التواجد والإستمرارية : ويقصد بها توفر المعلومات متى ما تم الحاجة إليها ومن ثم إمكانية الإستفادة منها من خلال قنوات أمنية سليمة، مثال على ذلك: تعطل القرص الصلب في الحاسوب مما يؤدي إلى تعذر الوصول إلى المعلومات والاستفادة منها أو تعطل نظام معلوماتي كامل على مستوى أكبر، إذًا الإستمرارية عنصر مهم ذات تأثير جذري على أمن المعلومات ينبغي توفرها في أنظمة المعلومات .

وينبغي التنويه إلى إن هذه العناصر هي أهم الركائز في مفهوم أمن المعلومات، وقد نجد بعض العلماء يزيد عناصر أخرى تدعم هذا المفهوم[7].

2/ المخاطر الحديثة التي تواجه أنظمة المعلومات :

لقد أصبح اختراق أنظمة المعلومات ونظم الشبكات والمواقع المعلوماتية خطراً يقلق العديد من المؤسسات في السنوات الأخيرة ومع مرور الزمن نجد بالرغم من سبل الحماية التي تتبعها المؤسسات، إلا أن هناك ارتفاعا واضحا في معدل الإختراقات مع تنوع الوسائل المستخدمة في الإختراق أما عن طبيعة الأخطار التي يمكن أن تواجهها نظم المعلومات فهي عديدة، فالبعض منها قد يكون مقصود كسرقة المعلومات أو إدخال الفيروسات وغيرها وهي الأشد ضررا على نظم المعلومات، كما يكون مصدرها أحيانا من داخل أو خارج المؤسسة، وقد يصعب أحيانا التنبؤ بالدوافع العديدة للأشخاص الذين يقومون بها، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية والكوارث الطبيعية.

1/2- أخطار نظم المعلومات:

عندما يتم تخزين كميات كبيرة من البيانات في شكل إلكتروني، فهي عرضة لأنواع كثيرة من التهديدات، من خلال شبكات الإتصالات، فالترابط بين نظم المعلومات والمواقع المختلفة، يمكن يؤدي بدخول لأشخاص غير مرخص لهم، وبالتالي يمكن أن يحدث سوء المعاملة، أو الغش في أي لحظة تصلها الشبكة، فمن الممكن الوصول إلى البيانات المتدفقة عبر الشبكات، وسرقة البيانات القيمة أثناء الإرسال، أو تغيير الرسائل دون إذن.

كما يمكن تعطيل شبكة في نقاط مختلفة، كذلك يمكن إطلاق المتسللين هجمات الحرمان من الخدمة أو البرامج الضارة لتعطيل تشغيل المواقع على شبكة الإنترنت، كل هذه الأخطار قادرة على اختراق أنظمة المؤسسات وتدمير أو تغيير بيانات المؤسسات المخزنة في قواعد البيانات أو الملفات.

ففي سنة 2009، حدد الخبراء الأمن 30 ثغرات أمنية في أنظمة التشغيل والبرامج من الهواتف الذكية التي قدمتها شركة آبل ونوكيا وبلاك بيري، وحتى التطبيقات التي تم تطويرها خصيصا للهواتف النقالة فهي قادرة على التحول إلى برمجيات خبيثة، على سبيل المثال، في ديسمبر 2009، سحبت جوجل عشرات من تطبيقاتها المصرفية عبر الهاتف المحمول من Android Market، لأن ذلك يُمكن أن يحدث سرقة أوراق الإعتمادات المصرفية للعملاء.

فيمكن للهواتف الذكية المستخدمة من قبل المديرين التنفيذيين للمؤسسات أن تحتوي على بيانات حساسة مثل أرقام المبيعات، وأسماء العملاء وأرقام الهواتف وعناوين البريد الإلكتروني...، وبالتالي يستطيع المتطفلين من الوصول والدخول إلى شبكات المؤسسات الداخلية من خلال هذه الأجهزة.

كذلك الشبكات العامة الكبيرة، مثل الأنترنت Internet، أكثر عرضة من الشبكات الداخلية internal لأنها مفتوحة لأي شخص تقريبا، فشبكة الإنترنت ضخمة جدا ويمكن أن يكون لها تأثير واسع النطاق إلى حد كبير، فعندما تكون شبكة الأنترنت جزءا من شبكة المؤسسة، تصبح نظم المعلومات في المؤسسة أكثر عرضة لأعمال الغرباء.

فكل أجهزة الكمبيوتر المتصلة بالأنترنت باستمرار من قبل أجهزة مودم الكبل أو خط المشترك الرقمي (DSL) والتي تعتبر خطوط أكثر انفتاحا على الإختراق من قبل الغرباء لأنها تستخدم عناوين الأنترنت الثابتة حيث يمكن التعرف عليها بسهولة، فعنوان الأنترنت الثابت يخلق هدفا للقراصنة.

كما أن البريد الإلكتروني E-mail قد يحتوي على المرفقات التي تكون كنقطة انطلاق للبرمجيات الخبيثة أو الوصول غير المصرح به إلى أنظمة المؤسسات الداخلية، كذلك يمكن للموظفين استخدام البريد الإلكتروني لإرسال رسائل أسرار تجارية قيمة، والبيانات المالية، أو معلومات سرية عن العملاء إلى المستلمين غير المصرح لهم.

2/2: أنواع الأخطار التي تتعرض لنظم المعلومات:

يمكن تصنيف الأخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات إلى ثلاث فئات[8] :

أ . الأخطاء البشرية Humane Errors

وهي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام، أو في عمليات تحديد الصلاحيات للمستخدمين، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة نظم المعلومات في المؤسسات، وتشمل المشاكل العرضية الناجمة عن كل من العاملين والموظفين، مثل: ذلك الموظف الذي يسيء فهم إجراءات التشغيل بطريق الخطأ فيحذف سجلات العملاء، مثال آخر، موظف يقوم أثناء النسخ الاحتياطي لقاعدة البيانات بتثبيت قاعدة بيانات قديمة على الحالية عن غير قصد.

ب . الأخطار البيئية Environmental Hazard

وتشمل الزلازل، العواصف، الفيضانات، الأعاصير والحرائق والمشاكل المتعلقة بأعطال التيار الكهربائي والإنهيارات الثلجية، وغير ذلك من أعمال الطبيعة، إضافة إلى المشاكل القائمة في تعطل أنظمة التكييف والتبريد

وغيرها، والتي تؤدي هذه الأخطار إلى تعطل عمل هذه التجهيزات وتوقفها لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات .

فالحوادث الطبيعية والكوارث هي مصدر للمشاكل الأمنية فمشاكل هذه الفئة تشمل ليس فقط الفقدان الأولي للقدرة والخدمات، ولكن أيضا الخسائر الناجمة عن إجراءات إسترداد النظام من المشكل الأولي (خطأ بشري في النسخ الإحتياطي).

ج. جرائم الحاسوب Computer Crime

تواجه أنظمة المعلومات بعض المشكلات الشائعة التي بدأت تغزو أنظمة المعلومات وتساهم في تدميرها أو تخريبها أو سرقة التخزين المعلوماتي المحفوظ في أجهزة الحاسوب، فيتم تعريف جرائم الحاسوب اليوم بأنها جريمة تنطوي على الحاسوب أو الشبكة، حيث بعض الجرائم تستهدف بشكل مباشر الحاسوب أو الشبكات، كما يمكن للجرائم الأخرى استخدام أجهزة الحاسوب و / أو الشبكات لإرتكاب الجريمة، كما أن بعض الهجمات تشمل جهاز حاسوب واحد، في حين يمكن إستهداف الآلاف منها[9].

ومع زيادة تواصل المؤسسات فيما بينها عبر الأنترنت، زادت الهجمات الإلكترونية cyberattacks والتي تمثل تحديا كبيرا لإدارة نظم المعلومات لما تسببه من خسارة كبيرة، فالجرائم المتعلقة بالحواسيب هي الجرائم التي تستخدم فيها الحواسيب كأداة لتنفيذ الجريمة، ويمكن أن تتم الجرائم المحوسبة سواء من قبل أشخاص خارج المؤسسة يقومون باختراق نظام الحاسوب (غالبا من خلال الشبكات) أو من قبل أشخاص داخل المؤسسة يملكون صلاحيات الدخول إلى النظام ولكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة، وتشير الدراسات التي أجرتها دائرة المحاسبة العامة وشركة Orkand للإستشارات إلى أن الخسائر الناتجة عن جرائم الكمبيوتر تقدر بحدود 1.5 مليون دولار لشركات المصارف المحوسبة في الولايات المتحدة الأمريكية، ومن ناحية أخرى يقدر المركز الوطني لبيانات جرائم الحاسوب في لوس أنجلوس بأن 70% من جرائم الكمبيوتر المسجلة حدثت من الداخل، أي من قبل من يعملون داخل المنظمات ، هذا و أن جرائم الحاسوب تزداد بصورة واضحة مما أصبحت تشكل تحديا خطيرا يواجه الإدارات العليا عموما و إدارة نظم المعلومات على وجه الخصوص .

إذن جرائم الحاسوب يمكن أن تكون من موظفين وعمال سابقين الذين دمروا عمدا بيانات أو مكونات النظام ، كما يتضمن المتسللين الذين يخترقون النظام من الخارج لسرقة البيانات لتحقيق مكاسبهم المالية، وحتى أنه يشمل الإرهاب السيبراني* Cyberterrorism، وكذلك صانعي البرمجيات الخبيثة التي تصيب أنظمة الحاسوب.

ويمكن وصف وتلخيص بعض التقنيات الأكثر شيوعا التي تستخدم لمهاجمة أجهزة الحاسوب وأنظمة المعلومات كما يلي:

الجدول 2-1: الهجمات الإلكترونية الأكثر شيوعا

بعض أنواع الهجمات الإلكترونية الشائعة	تعريفها
فيروس الكمبيوتر Computer Virus	عبارة عن وحدة صغيرة من التعليمات البرمجية التي تغزو برنامج الحاوسب أو الملف، وعند تنفيذ البرنامج أو فتح الملف المصاب، يقوم الفيروس بنسخ نفسه ليغزو البرامج والملفات الأخرى في الحاسوب. فتفعل أشياء سيئة كمحو الملفات وإفساد البرامج، وهكذا ينتقل الفيروس لجهاز آخر عبر الملفات والبرامج المصابة بالفيروسات.

	مثل: فيروس ILOVEYOU ماي 2000، فيروس مرفق في رسالة البريد الإلكتروني، حيث قدر الضرر بـ 10-15 مليار دولار.
الدودة Worm	فيروس لديه القدرة على نسخ نفسه من جهاز لآخر، ولكن عبر الشبكة. مثل: دودة Sobig.F أوت 2003، تنتشر عبر مرفقات البريد الإلكتروني، بإرسال كميات هائلة من البريد الإلكتروني بمعلومات مزورة؛ الضرر المقدر بـ 5-10 مليار دولار.
أحصنة طروادة Trojan Horse	برامج تقوم بكسر الأمن، يتم إدخالها في جهاز الحاسوب دون الإحساس بها، فقد تكون بطاقة تحية إلكترونية، شاشة توقف، أو لعبة، وتعمل كوسيلة لمتسلل يدخل للكمبيوتر لاحقا.
القنبلة المنطقية Logic Bomb	برامج أدخلت في جهاز الحاسوب الذي تم تصميمه لاتخاذ إجراءات في وقت معين أو عندما يحدث حدث معين.
هجمات حجب الخدمة Denial of Service Attack	عدد كبير من أجهزة الحاسوب على الأنترنت ترسل في نفس الوقت رسائل متكررة لحاسوب مستهدف، مما يؤدي إلى التشويش على الجهاز وخطوط الإتصالات وبالتالي حرمان المستخدم من الحصول على الخدمة.

Source : Carol V. Brown, op.cit, p :562.

إن أنواع الخسائر الناجمة عن جرائم الحاسوب computer crimes (البعض يسميها الجرائم الإلكترونية e-crimes) أن تتخذ أشكالا عديدة، فالعديد من الإختراقات تنطوي على البيانات، مثل فقدان البيانات الطبية أو البيانات المالية للأفراد، وخاصة بيانات بطاقة الإئتمان التي تشكل أكبر خرق لبيانات العملاء حتى الآن ويمس تجار التجزئة أو المؤسسات المالية، وخبراء الصناعة تشير لتقديرات إلى أن إجمالي الخسائر التجارية يمكن أن تقترب إلى مليار دولار سنويا.

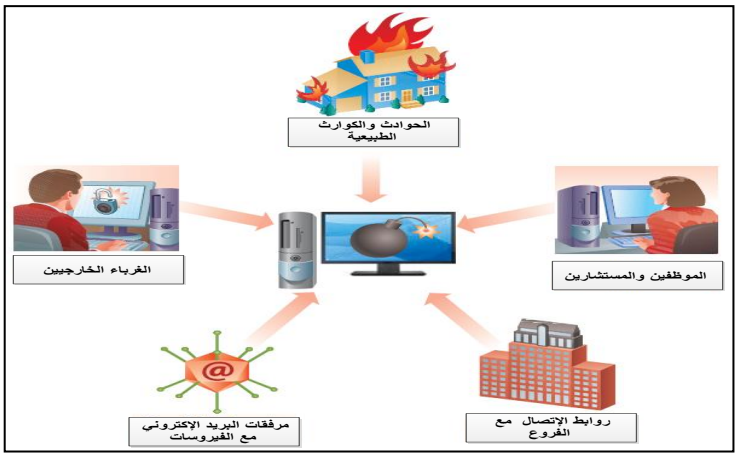
كما أن مرتكب جريمة الحاسوب يمكن أن يكون هاكر hacker أو كاسر cracker، فالقراصنة عادة لا تنوي ضرر على الإنسان، بل تبرر أعمالهم بأنها مفيدة في الإشارة إلى مواطن الضعف في ممارسات أمن الكمبيوتر أو منتجات برامج معينة، كالإحساس بالضيق مع هيمنة أنظمة تشغيل مايكروسوفت.

في المقابل، الكاسر يستخدم تقنيات القرصنة عمدا لسرقة المعلومات، القضاء على محركات الأقراص الصلبة، أو على ضرر الآخرين، بما في ذلك الهجمات على الحكومات، وعلى الرغم من الغرباء تشكل أكبر خطر أمني للمؤسسات إلا أن المطلعين (الموظفين الحاليين والموظفين السابقين) لا تزال مستمرة لتكون مصدرا لجريمة الكمبيوتر في حوالي 20 % من الحوادث.

كما أن الجرائم الداخلية التقليدية كالوصول غير المصرح به إلى أنظمة المعلومات، أو الشبكات، أو سرقات حقوق الملكية الفكرية والأسرار التجارية، والبحث وتنمية المعرفة من قبل الموظفين المصرح لهم من الوصول إلى المعلومات التي يتم سرقتها، لهذا العديد من المؤسسات تحاول تقليل هذا النوع من المخاطر عن طريق إلغاء كلمات المرور على الفور من حاسوب الموظف الذي يستقيل أو المنتهية مهامه.

مصدر آخر متزايد من الجريمة الإلكترونية هو شركاء الأعمال للمؤسسات، والذين لديهم القدرة للوصول إلى مصادر المعلومات الخاصة بهم بما في ذلك مؤسسات تقنية المعلومات، الموردين الآخرين، والإستشاريين، والمقاولين...، فالدراسات الحالية تبين أن خروقات البيانات التي يعاني منها العملاء يتورط فيها الشركاء التجاريين.

كما أن عولمة الأعمال يجلب أيضا زيادة مخاطر أمن المعلومات من الشركاء التجاريين، على سبيل المثال، العديد من المؤسسات تدخل في مشاريع مشتركة أو التحالفات الإستراتيجية الأخرى للبحث والتطوير، تصنيع المنتجات الجديدة، أو اختبار المنتج، والتي أصبحت من المصادر الخارجية، كذلك شركات تجهيز كشوف المرتبات للمؤسسة أو بيانات المطالبات، كما أن بعض المؤسسات تستخدم خدمة التزويد بخدمات الأنترنت وتخزين بيانات العملاء للمؤسسات، فكل هذه الترتيبات للشريك التجاري تزيد من مخاطر أمن المعلومات.



أما Valacich & Schneider (2012)، فبينا التهديدات التي يتعرض لها نظام المعلومات في الشكل التالي:

الشكل 2-1 : أهم التهديدات التي يتعرض لها نظام المعلومات

Source : Joe Valacich, Christoph Schneider, OP.CIT, p :401

فالتهديدات الرئيسية لأمن نظم المعلومات هي كالتالي[10]:

- **الكوارث الطبيعية**. انقطاع التيار الكهربائي، والأعاصير، والفيضانات، ...الخ.
- **الحوادث**. انعدام الخبرة أو الإهمال لمستخدمي الحاسوب.
- **الموظفين والمستشارين**. الأشخاص داخل المؤسسة الذين لديهم إمكانية الوصول إلى ملفات إلكترونية.
- **روابط الإتصالات الخارجية**. يمكن للمعلومات الإلكترونية تكون في خطر عندما تنتقل بين فروع المؤسسة.
- **الغرباء**. الهاكرز والكاسر الذين يخترقون الشبكات وأنظمة الحاسوب للتجسس أو لإلحاق الضرر (الفيروسات).

بالنسبة للأفراد وكذلك المؤسسات، يمكن محاولة التعافي من الكوارث أن تكلف الكثير من الوقت والمال، إضافة إلى إمكانية فقدان المؤسسات لكثير من سمعتها إذا أنظمتها أصبحت غير متوفرة أو معطلة بسبب القراصنة،

وبالتالي، بالنسبة للمؤسسات، من الضروري حماية أنظمتها من النشاط الإجرامي، وضمان استمرارية الأعمال من خلال تأمين البنية التحتية الخاصة بنظام المعلومات لديها[11].

3/ الحماية من أخطار نظم المعلومات :

تعتبر عملية الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة والصعبة والتي تتطلب من إدارة نظم المعلومات الكثير من الوقت والجهد والموارد المالية وذلك للأسباب التالية [12]:

أ. العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات .
ب. توزع الموارد المحوسبة على العديد من المواقع التي يمكن أن تكون أيضا متباعدة .
ج. وجود التجهيزات المحوسبة لدى أفراد عديدين في المؤسسة وأحيانا خارجها .
د. صعوبة الحماية من الأخطار الناتجة عن ارتباط المؤسسة بالشبكات الخارجية .
ه. التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها.
و. التأخر في اكتشاف الجرائم المحوسبة مما لا يتيح للمؤسسة إمكانية التعلم من التجربة والخبرة المتاحة.
ز. تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المؤسسات تحملها .

هذا وتقع مسؤولية وضع خطة الحماية للأنشطة الرئيسية على مدير نظم المعلومات في المؤسسة على أن تتضمن هذه الخطة إدخال وسائل الرقابة التي تضمن تحقيق ما يلي:

- الوقاية من الأخطار غير المتعمدة .
- الوقاية من إعاقة أو صنع الأعمال التخريبية المتعمدة .
- اكتشاف المشاكل بشكل مبكر قدر الإمكان .
- المساعدة في تصحيح الأعطال واسترجاع النظام .

ويمكن تصميم نظام الرقابة ضمن عملية تطوير نظام المعلومات ويجب أن يركز هذا النظام على مفهوم الوقاية من الأخطار، ويمكن أن يصمم لحماية جميع مكونات النظام بما فيها التجهيزات والبرمجيات والشبكات .

1/3 : العناصر الأساسية لنظام الأمن المعلوماتي :

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

أ. منظومة الأجهزة الإلكترونية وملحقاتها :

إن أجهزة الحاسوب تتطور بشكل مقابل هناك تطور في مجال السبل المستخدمة لإختراقها مما يتطلب تطوير القابليات والمهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب والعبث المقصود في الأجهزة أو غير المقصود .

ب. الأفراد العاملين في أقسام المعلومات :

يلعب الفرد دورا أساسيا و مهما في مجال أمن المعلومات والحواسيب وله تأثير فعال في أداء عمل الحواسيب بجانبيه الإيجابي والسلبي، فهو عامل مؤثر في حماية الحواسيب والمعلومات ولكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة وسرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير، لذا من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين ووضع تعليمات واضحة لاختيارهم وذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد إضافة إلى وضع الخطط لزيادة الحس الأمني والحصانة من التخريب، كما يتطلب الأمر المراجعة

الدورية للتدقيق في الشخصية والسلوكية للأفراد العاملين من وقت لآخر وربما يتم تغيير مواقع عملهم ومحاولة عدم احتكار المهام على موظفين محدودين .

ج. البرمجيات المستخدمة في تشغيل النظام :

تعتبر البرمجيات من المكونات غير المادية وعنصر أساسي في نجاح استخدام النظام، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية ويمكن 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 وكتابة برامجه من خلال وضع عدد من الإجراءات كالمفاتيح والعوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها وتمنع أي شخص من إمكانية التلاعب والدخول إلى النظام وذلك من خلال أيضا تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها، و محاولة التميز بين اللذين يحق لهم الإطلاع وحسب كلمات السر الموضوعة، و هناك أسلوبان للتمييز إما عن طريق البرمجيات أو استخدام الأجهزة المشفرة .

د. شبكة تناقل المعلومات :

تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الإتصالات كما أنها سهلت عملية التراسل بين الحواسيب وتبادل واستخدام الملفات، ولكن 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 وضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات وتوفير الأجهزة الخاصة بالفحص، كما أن نظم التشغيل المستخدمة والمسؤولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة وقدرة عالية على الكشف عن التسلل إلى الشبكة وذلك من خلال تصميم نظم محمية بإقفال معقد أو عن طريق المشفرات وربطها بخطوط الإتصال والتي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة ومعدات لغرض تشفير تناقل المعلومات أو الملفات .

ه. مواقع منظومة الأجهزة الإلكترونية وملحقاتها :

يجب أن تعطى أهمية للمواقع والأبنية التي تحتوي على أجهزة الحواسيب وملحقاتها، وحسب طبيعة المنظومات والتطبيقات المستخدمة يتم إتخاذ الإجراءات الإحترازية لحماية الموقع وتحصينه من أي تخريب أو سطو وحمايته من الحريق أو تسرب المياه والفيضانات، ومحاولة إدامة مصدر القدرة الكهربائية وانتظامها وتحديد أساليب وإجراءات التفتيش والتحقق من هوية الأفراد الداخلين والخارجين من الموقع وعمل سجل لذلك.

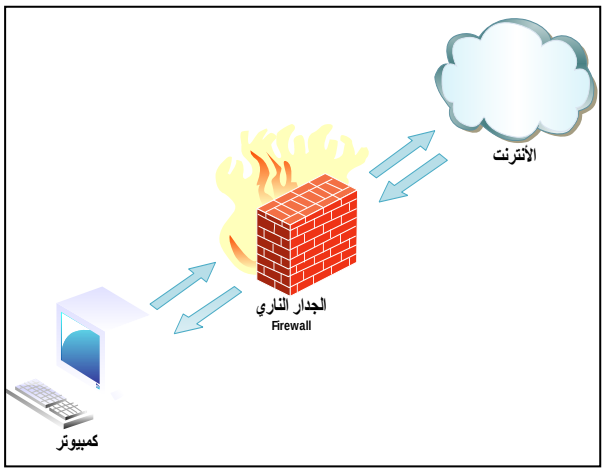
2/3- حماية المعلومات والعمليات التجارية:

معظم الأفراد تذكر الأجهزة والبرامج في إجاباتهم عن الوسائل المستعملة في الحماية، على سبيل المثال، جدران الحماية Firewalls ، والتشفير Encryption ، ومكافح الفيروسات Antivirus ، مضاد البريد المزعج Antispam ، مكافح التجسس Anti-spyware ، ومكافح التصيد الإحتيالي Anti-phishing، ...الخ.

فالجدران النارية وأنظمة كشف التسلل هي في شتى الشبكات لرصد ومراقبة حركة المرور من وإلى الشبكة، كما هو مبين في الشكل التالي:

الشكل 3-1: الجدار الناري للمؤسسة

Source : Kenneth, Laudon, Essentials of Management Information Systems, 8 E, Pearson, USA, 2009. P :278.



بالتأكيد، كل هذه الوسائل تعتبر دفاعات تكنولوجية ضرورية، لكنها غير كافية لأن حماية البيانات والعمليات التجارية تشمل ما يلي[13]:

• جعل البيانات والوثائق متاحة الوصول إليها 7 أيام /24ساعة مع تقييد الوصول إليها في وقت واحد.

• تنفيذ وتطبيق إجراءات وسياسات استخدام مقبولة لشركة مملوكة للبيانات، والأجهزة، والبرمجيات، والشبكات.

• تشجيع تبادل آمن وقانوني للمعلومات فيما بين الأشخاص المخولين والشركاء.

• ضمان الإمتثال للوائح والقوانين الحكومية.

• منع الهجمات من خلال وجود شبكة دفاعات التسلل في المكان المناسب.

• كشف وتشخيص، والرد على الحوادث والهجمات بشكل فوري.

• الحفاظ على الضوابط الداخلية لمنع التلاعب في البيانات والسجلات.

• الإسترداد من الكوارث وبسرعة في حالة وجود عطل في الأعمال التجارية.

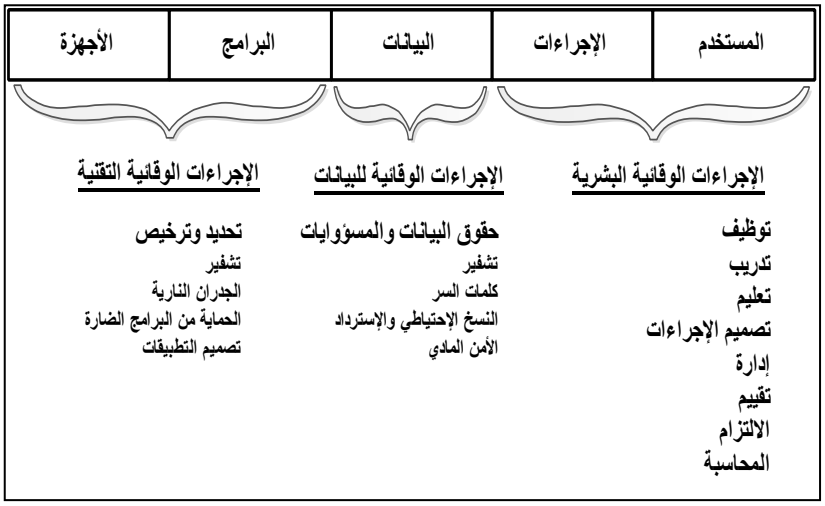
كما أن سياسات الأعمال، والإجراءات، والتدريب، والإسترداد من الكوارث وكذلك خطط التكنولوجيا كلها أمور تلعب دورا حاسما في أمن نظم المعلومات، فأمن نظم المعلومات يغطي حماية المعلومات، وشبكات الإتصالات، وعمليات التجارة الإلكترونية لضمان السرية الخاصة، والسلامة، والتوفر، والإذن بالإستخدام.

خلال سنة 2010، مجرمي الأنترنت أطلقوا أكثر من 100 هجوم / في الثانية على أجهزة الكمبيوتر في جميع أنحاء العالم، وفقا لتقرير صادر عن أمن تكنولوجيا المعلومات لشركة سيمانتيك[**]، والتي حددت تقريبا 2.9 مليون شفرات خبيثة خلال فترة 12 شهرا.

كما يجب على المؤسسات معالجة الأمن بطريقة تأمين العناصر الخمسة لنظام المعلومات، كما هو مبين في الشكل 3-2، بعض وسائل الحماية تشمل أجهزة الحاسوب والبرمجيات، والبعض تنطوي على البيانات؛ وإشراك

الإجراءات والأفراد الآخرين، بالإضافة إلى هذه الإجراءات، والضمانات يجب أيضا النظر في إجراءات التعافي من الكوارث، فبرنامج أمني فعال يتكون من رصيد الإجراءات من جميع هذه الأنواع.

الشكل 3-2: الإجراءات الوقائية لعناصر أنظمة المعلومات



Source : David M. Kroenke, OP.CIT, p :286

3/3- المعايير الدولية لأمن نظم المعلومات:

لمساعدة المؤسسات في إدارة أمنها المعلوماتي فقد تم استحداث العديد من المعايير الدولية، وهي بمثابة الحد الأدنى من الضوابط الأمنية التي يوصي بها خبراء الأمن المعلوماتي، في هذا الإطار من المفيد الإطلالة المختصرة على ما أنتجته الجهود الدولية في هذا المجال والإستفادة من الخبرات المتراكمة في هذا الصدد .

فقد أصدرت المنظمة العالمية للتقييس المواصفة الدولية ISO 27001 والتي تعتبر أحد سلسلة عائلة المعايير ISO/ 27000: 2009 الصادرة عن المنظمة العالمية للتقييس، وهو يوصف الإحتياجات إلى إنشاء وتشغيل ومراقبة ومراجعة وتحسين نظام إدارة وصيانة معلومات موثق أمن باستخدامه منهاج التحسين المستمر، هذا المعيار لا يفرض كما قد يظن البعض ضوابط أمنية معينة أو يعالج فقط النواحي الأمنية لتقنية المعلومات، بل أنه يقف فقط عند مستوى إدارته للنظام، أما من يقوم بدور إرشادي لتفسير وتطبيق الضوابط المعرفة في ملحقه فهو معيار قواعد الممارسة لإدارة أمن المعلومات ISO 27002 المنتمي إلى نفس العائلة والذي من المقصود استخدامه سوياً[14].

وكما يعنى هذا المعيار إلى إنشاء نظام إدارة أمن معلومات يدار من خلاله المخاطر الأمنية، فإن المؤسسات تسعى من خلال اثباتها لإدارة نظامها وضوابطها الأمنية وفق توصيفات النظام الحصول على شهادة أمن معترف بها

دولياً، ومع وجود هذا النظام يكون بمقدور الإدارة العليا للمؤسسة التحكم ومراقبة الأمن كما باستطاعتها التخفيف من وطأة المخاطر المحيطة بعملها.

ومنه فإن مجموعة معايير ISO 27000 ضمن المنظمة العالمية للتقييس تهدف لتلائم استخدامات متنوعة كالتالي[15]:

- يستخدم داخل المؤسسات لتشكيل الأهداف والمطالب الأمنية .
- التوافق مع التشريعات والقوانين .
- التعرف على إجراءات جديدة لإدارة أمن المعلومات .
- يستخدم من قبل الإدارة لتحديد وضعية النشاطات الأمنية .
- يحدد المدققين الداخليين والخارجيين من خلاله مستوى التوافق مع السياسات والإجراءات المقررة

إن معيار قواعد ممارسه أمن المعلومات ISO 27002 يتطابق في هيكليته مع مرفق -أ- من ISO 27001 لكنه أكثر تفصيلاً من حيث المضمون، فهو يسهب في شرح كيفية تطبيق الضوابط الأمنية عند اختيارها، إنه من الممكن استخدام كل أو جزء من هذا المعيار منفصلاً عن ISO 27001 في أي مؤسسة تسعى وراء رفع مستواها الأمني عبر اختيار الضوابط الأمنية المناسبة لتصدي الأخطار المحيطة، مع العلم أنه ليس هناك أولويات أو تسلسل عند انتقاء الضوابط، وكما تنبه المنظمة الدولية إليه فإنه لا يتحقق الأمن الكامل بمجرد العمل بهذه الضوابط بل أنها تحث على تدخل إضافي من المؤسسة لرصد وتقييم وتحسين فعالية الضوابط الأمنية الداعمة لأهدافه.

كما أن فوائد تطبيق معيار ISO / 27001 تتلخص في[16]:

- المحافظة على ممتلكات المؤسسة سواء كانت معنوية مثل المعلومات والبرامج أو المادية كالأجهزة والمباني.
- زيادة الوعي لجميع موظفي المؤسسة بأهمية أمن المعلومات والنتائج السلبية المترتبة بعدم الإلتزام بذلك.
- الإلتزام بمعيار ISO 27001، وبالمواصفات عموما دليل على اهتمام المؤسسة بتطوير أدائها وحرصها على الإلتزام بأعلى المعايير لتقديم أفضل السلع والخدمات.
- زيادة التنافسية للمؤسسة مقارنة بالمؤسسات الأخرى العاملة في نفس المجال.
- جاهزية المؤسسة على مواصلة أدائها في حالة حصول الحوادث الطارئة الطبيعية.

الخلاصة:

قضية أمن المعلومات وتبادلها عبر الشبكات من القضايا التي تشغل بال ليس فقط الباحثين والمختصين، بل المنظمات الدولية والعالم المرتبط بها، نظرًا للأهمية الفائقة لتقنيات المعلومات في شتى مجالات الحياة في هذا العصر.

فتعتبر المعلومات عنصرا أساسيا لأعمال أي مؤسسة وبالتالي يتوجب حمايتها بانتظام، وإن هذه الحماية يتعاظم دورها خاصة في ظل عالمنا اليوم الذي يتمتع ببيئة ذات أعمال مترابطة ومتسارعة الخطى مما يزيد من حجم التهديدات والمخاطر.

ولاشك أن تزايد الإعتماد على المعلومات وشبكاتها يزيد أيضًا من تأثير الأخطار التي يمكن أن تواجهها، فلابد من السعي إلى مواجهة هذه الأخطار والإهتمام بتطوير الأساليب والوسائل التقنية اللازمة لهذه المواجهة، إضافة إلى إيجاد أفضل القواعد الإدارية التي تساهم في دعم هذه المواجهة، من أجل الحد من الأخطار المحتملة، بل والسعي إلى التخلص منها.

التوصيات:

- العمل على تحقيق العناصر الأساسية لأمن المعلومات (السرية، التكاملية، والإستمرارية).
- تقييم المخاطر المحتملة بشكل دوري للدراية بما يجب عمله عند حدوث مشكل لأمن نظم المعلومات.
- إشراك العاملين وتوعيتهم في مجال أمن نظم المعلومات.
- تخصيص إدارة لأمن نظم المعلومات، وهذا لتطبيق الأمن المعلوماتي في المؤسسات.
- السعي للحصول على معيار ISO 27001، فهو التطبيق الأمثل لأمن نظم المعلومات في المؤسسات.

كما يجدر بنا القول أن مسألة تحقيق أمن نظم المعلومات بشكل كامل وبنسبة 100 % لا يمكن ضمانها، لأن مجال التقنية عبارة عن بيئة متغيرة تجلب لنا كل جديد وفي كل لحظة مخاطر جديدة غير محدودة، لذلك ينبغي أن يكون هدفنا هو الحفاظ قدر الإمكان على أمن المعلومات ومتابعة كل ما هو جديد في عالم التكنولوجيا .

قائمة المراجع:

[1]: الدليل العربي لأمن المعلومات، المؤتمر الثاني لأمن المعلومات الإلكترونية مسقط، . www.arabicitsecurity.com/2016/06/20

[2]: دلال صادق، حميد ناصر الفتال، أمن المعلومات، دار اليازوري، الأردن، 2008. ص:11.

[3]: Kenneth C. Laudon, Jane P. Laudon, Management Information Systems Managing The Digital Firm, Twelfth Edition, Prentice Hall, USA, 2012. p :293.

[4]: المركز القومي للمعلومات- الإدارة الفنية، قسم الجودة والتطوير- وحدة المعايير، لجنة معايير نظم التشغيل والسرية والتأمين، معيار قواعد الممارسة لإدارة أمن المعلومات، الطبعة الثانية، السودان، فيفري 2010. ص:7.

[5]: Effy Oz, Management Information Systems Sixth Edition, Cengage, USA, 2009. p :475.

[6]: آلاء سعد العلي، الوعي الأمني لدى المجتمع السعودي، مركز التميز لأمن المعلومات، المملكة العربية السعودية، دون سنة النشر. ص:4.

[7]: منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، مصر، 2006. ص:13.

[8]: David M. Kroenke, Experiencing MIS, Third Edition, Prentice Hall, USA, 2012. p :282.

[9]: Carol V. Brown, Daniel W. DeHayes, Jeffrey A. Hoffer, E. Wainright Martin, William C. Perkins, Managing Information Technology, Seventh Edition, Prentice Hall, USA, 2012. P :561.

[*]: هو إرهاب العالم الإلكتروني Cyber Terrorism ، وهي هجمات تستهدف نظم الكمبيوتر والمعطيات لأغراض دينية أو سياسية أو فكرية أو عرقية وفي حقيقتها تعتبر جرائم إتلاف للنظم والمعطيات أو جرائم تعطيل للمواقع وعمل الأنظمة.

[10]: Joe Valacich, Christoph Schneider, Information Systems Today Managing in the Digital World, Fifth Edition, Prentice Hall, USA, 2012. P :400.

[11]: عوض حاج على أحمد، عبد الأمير خلف حسين، أمنية المعلومات وتقنيات التشفير، دار الحامد، الأردن، 2005. ص:20.

[12]: Stuart Jacobs, Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance, John Wiley & Sons, Canada, 2011. P : 427.

[13]: Efraim Turban, Linda Volonino, Information Technology for Management Improving Strategic and Operational Performance, 8 ed, John Wiley & Sons, Inc, USA, 2011. P :124.

[**]: شركة أمريكية تأسست منذ 1982، تقدم خدمات حماية المعلومات للشركات، للمزيد اطلع على الموقع الرسمي www.symantec.com

[14]: Randall J. Boyle, Raymond R. Panko, Corporate Computer Security, 2 Ed, Prentice Hall, USA,2010. p :122.

[15] Stuart Jacobs, op.cit, p :170.

[16]: منصور عوض الحربي، مقالات أمن المعلومات، المملكة العربية السعودية، تاريخ 2016/09/12 -www.coeia.edu.sa/index.php/ar/invitations/invitation-to participate.html