دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

العنوان:	استراتيجية أمن المعلومات
المصدر:	مجلة أبعاد اقتصادية
الناشر:	جامعة أمحمد بوقرة بومرداس - كلية العلوم الاقتصادية والتجارية وعلوم التسيير
المؤلف الرئيسي:	قدايفة، أمينة
المجلد/العدد:	ع6
محكمة:	نعم
التاريخ الميلادي:	2016
الصفحات:	160 - 178
رقم MD:	916422
نوع المحتوى:	بحوث ومقالات
اللغة:	Arabic
قواعد المعلومات:	EcoLink
مواضيع:	أمن المعلومات، السياسة الأمنية، الجرائم الإلكترونية
رابط:	http://search.mandumah.com/Record/916422

© 2021 دار المنظومة. جميع الحقوق محفوظة.
هذه المادة متاحة بناء على الإتفاق الموقع مع أصحاب حقوق النشر، علما أن جميع حقوق النشر محفوظة. يمكنك تحميل أو طباعة هذه المادة للاستخدام الشخصي فقط، ويمنع النسخ أو التحويل أو النشر عبر أي وسيلة (مثل مواقع الانترنت أو البريد الالكتروني) دون تصريح خطي من أصحاب حقوق النشر أو دار المنظومة.

استراتيجية أمن المعلومات

Strategy of Information Security

د/ قدايفة أمينة *

أستاذة محاضرة قسم ب

جامعة أمحمد بوقرة بومرداس

الملخص

المعلومات هي من أهم الموجودات الضرورية في أي مؤسسة؛ لذا فإن هناك حاجة لحمايتها والتأكد من خصوصيتها وتكاملها وتوافرها، ومن أهم عوامل الحفاظ على أمن المعلومات هو وضع سياسات وإجراءات كافية لحمايتها.

إستراتيجية الأمن هي الأساس لأمن المعلومات في أي منظمة؛ فالسياسة المكتوبة والمنفذة بشكل جيد تحتوي معلومات كافية لما يجب عمله لحماية المعلومات والعاملين في المنظمة، وإستراتيجية الأمن كذلك تؤسس قواعد استخدام الحاسب للموظفين فيما يتعلق بمهامهم الفعلية.

يجب أن يقر مدير المنظمة بحقيقة وجود المخاطر الأمنية وكيفية تجنبها؛ فتنفيذ السيطرة والمراقبة يتطلب خطة محكمة، بالإضافة إلى تفاعل جميع موظفي المنظمة، والذي سيؤدي بدوره إلى نجاح إدارة أمن المعلومات. إن الهدف من صياغة إستراتيجية الأمن وتنفيذها هو تحسين توافر المعلومات وتكاملها، وخصوصيتها كذلك من داخل وخارج المنظمة. وسيُتطرق في هذه الدراسة إلى ماهية أمن المعلومات، ومن ثم سيُوضح مفهوم، وأهمية، وأهداف أمن المعلومات وأركانها، وبعد ذلك سيُتطرق إلى بعض المخاطر التي تتعرض لها العمليات الإلكترونية وكيفية الحماية منها، وفي النهاية ستُذكر ماهية إستراتيجية أمن المعلومات من خلال التطرق إلى مفهوم، وأهداف، وخصائص ومنطلقات إستراتيجية أمن المعلومات، ومكونات وخطوات بناء الإستراتيجية الأمنية، التي تعطي الخطوة الصحيحة لتطبيق الحماية الأمنية للمعلومات.

الكلمات المفتاحية: المعلومات، أمن المعلومات، المخاطر، السياسة الأمنية، استراتيجية أمن المعلومات.

* **kedaifa_imene1@yahoo.fr**

Abstract:

Information is the most important asset in any project, therefore there is a need to protect and ensure its privacy, integrity and availability. The most important factors in developing and maintaining information security are the development of policies and procedures for its protection. Security Strategy is fundamental for information security in any organization, so the written and the executed policy should contains sufficient information about what must be done to protect the information and employees in the organization. Even the security strategy establishes the rules for using the computer by employees regarding their actual duties.

Managers of organizations must approve the fact that security risks exist and that is necessary to avoid them, control and supervising execution require a consistent plan, in addition to the interaction of all the staff of the organization in this, which in turn will lead to the success of information security management.

Therefore, the aim of the establishment and implementation of the security strategy is to improve the availability of information, and its integrity and its privacy, inside the organization and outside it.

In this study, we will analyze the information security and clarify it and present its importance, its objectives and its elements. Then, we will show some risks facing the information security and propose some solutions. Finally, we will illustrate the elements of strategy of information security through the determination of its concept, its objectives, its properties and its requirements, and the presentation of components and steps of the conception of security strategy which ensure the protection of the information.

Key-Words: Information, Information Security, Risks, Security Policy, Strategy of Information Security.

المقدمة العامة

إن مناقشة الأمن في ظل هذه التطورات التقنية ليس بالأمر السهل، ومصطلح أمن المعلومات مفهوم شامل يحتوي عدة أمور، منها أمن الشبكات، وأمن الأجهزة المستخدمة، وأمن المنظمات، والأمن القانوني. ولوضع تصور شامل لحماية وأمن المعلومات لا بد أن نأخذ في الحسبان الإستراتيجية الأمنية (أمن الأجهزة والأدوات، أمن الشبكات، الأمن المنظم، الأمن القانوني). والإستراتيجية الأمنية تعتبر الغطاء الأمني لجميع الجوانب الأمنية، وهي التي تعطي كيفية إنجاز الأمن، ويجب بناؤها على المتطلبات وليس على الاعتبارات التقنية. والأهداف السياسية لأي إستراتيجية أمنية يجب أن تكون لإبقاء السرية والسلامة والكمال والتوفر لكل أصول الثروة المعلوماتية للشركات واتصالاتها. وتشير السرية إلى المعلومات السرية التي لا يراها إلا البعض مثل: المديرون، والمشرفون، وبعض المستخدمين. وهذه المعلومات يجب أن تبقى خاصة بالمنظمة، وببعض المستخدمين ضمن الشركة، وهي أيضاً تحفظ المعلومات من الاطلاع والكشف غير المخول أو المفاجئ. وتشير السلامة والكمال إلى معلومات وبيانات المنظمة، ومن المهم أن تكون دقيقة وحديثة جداً. والتكامل أو السلامة تحمي المعلومات من التعديل غير المخول أو المفاجئ. وأخيراً التوفر، ويشير إلى الوصول إلى معلومات ومصادر المنظمة، ومن المهم جداً أن تكون المعلومات ومصادر المنظمة متوفرة بسهولة. والتوافر يضمن الوصول الموثوق فيه للبيانات متى وأينما دعت الحاجة لذلك، ويجب على الإستراتيجية الأمنية أن تضع في الحسبان هذه الأهداف الثلاثة عند دراسة أي تهديدات محتملة للمنظمة.

وعلى إثر ذلك يمكن التطرق إلى الإشكالية التالية:

كيف يمكن تبني إستراتيجية أمنية ضرورية ولازمة لحماية أمن المعلومات في المنظمة؟

وللإجابة عن هذه الإشكالية، وجب علينا توضيح جملة من التساؤلات الفرعية، والتي نوجزها كالآتي:

1- ما هو المعيار الحقيقي لنجاح الأعمال بشكل إلكتروني؟

2- ما هي أهم المخاطر الالكترونية التي تعترض المنظمة في ظل استخدامها الواسع لتقنية المعلومات؟

3- ماهي وسائل توفير أمن المعلومات في المنظمة؟

4- ماهي مختلف الإجراءات الحماية لمكافحة أشكال الاقتحام الالكتروني؟

5- ما العناصر اللازم توافرها بالمنظمة في حالة بناء إستراتيجية أمن المعلومات؟

وللإجابة عن هذه التساؤلات الفرعية ارتأينا وضع مجموعة من الفرضيات، وهذا من أجل الإلمام بالموضوع:

1- المعيار الحقيقي لنجاح الأعمال بشكل إلكتروني هو مستوى أمن المعلومات الذي يمكن أن يقدمه، خصوصاً للتطبيقات والعمليات الحساسة.

2- تتعرض المنظمة إلى مشاكل إلكترونية جمة مرتبطة باستخدامها الوسائط الالكترونية.

3- يعتبر توفير أمن المعلومات في المنظمة تحديا هاما يستوجب توفير كامل الإمكانات البشرية والمادية.

4- تتخذ المؤسسة عدة إجراءات الحماية في ظل إستراتيجية معينة لمكافحة أشكال الاقتحام الالكتروني.

5- إن صياغة إستراتيجية الأمن وتنفيذها هو تحسين توافر المعلومات وتكاملها، وخصوصيتها كذلك، من داخل وخارج المنظمة.

تهدف هذه الدراسة إلى تحقيق ما يلي:

1– التأكيد على أن أهمية أمن المعلومات للمنظمات هي حاجة ماسة وضرورية؛

2– تثقيف العاملين بأهمية الأمن في المنظمة وتدريبهم على ذلك؛

3– تقديم استنتاجات وتوصيات يمكن من خلالها مساعدة المنظمة على تبني إستراتيجية أمنية وتطبيقاتها، لمواجهة التهديدات والمخاطر بكفاءة وفاعلية.

أما **منهج البحث** الذي اعتمدت عليه فهو المنهج الوصفي التحليلي، وذلك من خلال الاستعانة بالمصادر العلمية ذات العلاقة بالموضوع، والوسائل الالكترونية الأخرى.

قمنا بتقسيم هذا البحث إلى مبحثين، بحيث تعرضنا في المبحث الأول إلى **ماهية أمن المعلومات**، وذلك من خلال أربعة مطالب، حيث

المطلب الأول: مفهوم أمن المعلومات.

المطلب الثاني: أهمية وأهداف أمن المعلومات.

المطلب الثالث: أركان أمن المعلومات.

المطلب الرابع: الأخطار والحماية منها.

المبحث الثاني تطرقنا فيه إلى **ماهية استراتيجية أمن المعلومات**.ويشمل أربعة مباحث هي:

المطلب الأول: مفهوم إستراتيجية أمن المعلومات.

المطلب الثاني: أهداف إستراتيجية أمن المعلومات.

المطلب الثالث: منطلقات وخصائص إستراتيجية أمن المعلومات.

المطلب الرابع: مكونات وخطوات استراتيجية أمن المعلومات.

المبحث الأول: ماهية أمن المعلومات

مع الانتشار الكبير والشديد لتكنولوجيا المعلومات والأعداد المتزايدة لمستخدميها أصبحت مسألة الأمن المعلوماتي قضية بذاتها، تشكل أحد أبرز التحديات التي يواجهها الأفراد والمنظمات على حد سواء في عصر المعلومات.

سنتطرق في هذا المبحث إلى مفهوم أمن المعلومات وأهميتها وأهدافها وأبعادها، وأهم المخاطر والاعتداءات في بيئة الأعمال، والأخطار، والحماية منها.

المطلب الأول: مفهوم أمن المعلومات.

نظرًا للتدفق الهائل في حجم البيانات ولأهمية المعلومات أصبحت مشكلة حمايتها والحفاظ عليها موضع اهتمام العاملين والباحثين في هذا الميدان. وسوف نتناول مفهوم المعلومات قبل التطرق إلى مفهوم أمن المعلومات.

أولا: تعريف المعلومات:

هناك عدة تعاريف تناولت مفهوم المعلومات نذكر منها ما يلي:

تعرف المعلومات على أنها "بيانات تمّ تصنيفها بشكل يسمح باستخدامها والاستفادة منها، وبالتالي فالمعلومات لها معنى، وتؤثّر في ردود أفعال وسلوك من يستقبلها".[1]

من خلال هذا التعريف، يمكننا القول إنّ المعلومات تقيّم البيانات، وهذا يعني أنّها تشير إلى البيانات التي تمّ تقييمها مع موقف معيّن أو مشكلة تواجه فردا معيّنا لتحقيق هدف معيّن.

كما تعرف أيضا بأنها"نتائج عمليات النماذج، التكوين، التنظيم، أو تحويل البيانات بطريقة تؤدي إلى زيادة مستوى المعرفة للمستقبل".[2]

من خلال هذا التعريف، يمكننا القول إن المعلومات هي تلك البيانات التي تم إعدادها بعد تحليلها أو تفسيرها أو تجميعها في شكل له معنى، فتصبح لها قيمة ومنفعة، ويمكن تداولها ونشرها في صورة رسمية أو غير رسمية.

بصفة عامة، يمكننا القول: إنّ المعلومات هي كل ما يصل إلى علم الفرد، سواء أكان ذلك بالقراءة أم الاستماع أم المشاهدة، وتتعلق بجوانب وأمور تتّصل بحياة الإنسان والأوضاع المحيطة به، والعلاقات التي يقيمها، والظروف التي تلازمه، والإمكانات المتاحة له، والأحداث التي يواجهها من وقت لآخر.

ثانيا: تعريف أمن المعلومات

هناك عدة تعاريف تناولت مفهوم أمن المعلومات، نذكر منها ما يلي:

يعبر عن أمن المعلومات بأنه"الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية".[3]

أمن المعلومات هو كذلك"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".[4]

نستنتج من التعريفين السابقين، أن أمن المعلومات هو عبارة عن:

_ مجموعة من الاجراءات و التدابير الوقائية لحماية المعلومات؛

_ الهدف منها المحافظة على المعلومات والأجهزة والبرمجيات والأشخاص من التهديدات الداخلية والخارجية.

المطلب الثاني: أهمية وأهداف وأبعاد أمن المعلومات.

إن أمن المعلومات هي مجموعة الإجراءات والتدابير الوقائية التي تستخدم للمحافظة على المعلومات وسريتها من السرقة أو التلاعب أو الاختراق غير المشروع، لذلك سنحاول الآن تناول أهمية أمن المعلومات، وأهدافها، وأبعادها.

أولا: أهمية أمن المعلومات: تتمثل أهمية أمن المعلومات فيما يلي:

1. القطاعات الاقتصادية تعتمد على صحة ودقة المعلومات؛
2. حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق، تغطي المخاطر التي يمكن أن تظهر عند التعامل مع الأطراف الأخرى؛
3. الحاجة المتزايدة لإنشاء بيئة إلكترونية آمنة تخدم القطاعين الخاص والعام؛
4. النمو السريع في استخدامات التطبيقات الإلكترونية، والتي تتطلب بيئة آمنة؛
5. الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية، من أجل استمرارية الأعمال التجارية؛
6. مع تطور التقنية المعلوماتية وازدهارها توفرت فرص للإجرام الإلكتروني.

ثانيا: أهداف أمن المعلومات

إن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات–سواء من الناحية التقنية أم الأدائية–وكذا أهداف التدابير التشريعية في هذا الحقل، هو ضمان توفر العناصر التالية لأي معلومات يراد توفير الحماية الكافية لها:

1_ **السرية أو الموثوقية:** وتعني التأكد من أن المعلومات لا تنكشف، ولا يطلع عليها الأشخاص غير المخولين بذلك.

2_ **التكاملية وسلامة المحتوى:** التأكد بأن محتوى المعلومات صحيح، و لم يتم تعديله أو العبث به.

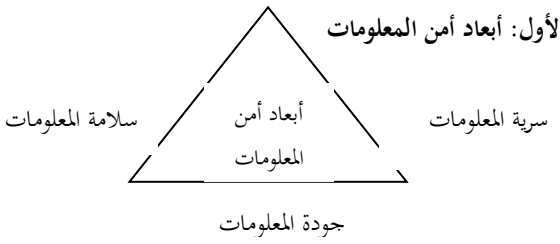
3_ **استمرارية وتوفر المعلومات أو الخدمة:** التأكد من استمرار عمل تكنولوجيا المعلومات، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.

4_ **عدم إنكار التصرف المرتبط بالمعلومات:** ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها أنه هو الذي قام بهذا التصرف، بحيث تتوفر القدرة على إثبات أن تصرفا ما قد تم من شخص ما في وقت معين.

ثالثا– أبعاد أمن المعلومات: تتمثل أبعاد أمن المعلومات في: (كما يوضحه الشكل الأول)

- **سرية المعلومات:** بمعنى عدم اطلاع أو تغيير المعلومات المخزنة على أجهزة الحاسوب أو المنقولة على الشبكة إلا من قبل الأشخاص المخولين بذلك.
- **سلامة المعلومات:** يتمثل ذلك في عدم تغيير المعلومات المخزنة على أجهزة الحاسوب أو المنقولة عبر الشبكة.
- **جودة المعلومات:** وذلك يتمثل في عدم حذف المعلومات المخزنة على أجهزة الحاسوب إلا من قبل الأشخاص المخولين بذلك.

الشكل الأول: أبعاد أمن المعلومات



المصدر: من إعداد الباحثة.

المطلب الثالث :أهم المخاطر والاعتداءات في بيئة الأعمال

تطال المخاطر والاعتداءات في بيئة المعلومات أربعة مواطن أساسية، هي مكونات تقنية المعلومات في أحدث تجلياتها:

- **الأجهزة:** كافة المعدات والأدوات المادية التي تتكون منها النظم، كالشاشات والطابعات ومكوناتها الداخلية، ووسائط التخزين المادية، وغيرها.

- **البرامج**: الأوامر المرتبة في نسق معين لإنجاز الأعمال، وهي إما مستقلة عن النظام أو مخزنة فيه.
- **المعطيات**: إنها الدم الحي للأنظمة، وما سيكون محلا لجرائم الكمبيوتر كما سنرى، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم. والمعطيات قد تكون في طور الإدخال أو الإخراج أو التخزين، أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط التخزين الخارجية.
- **الاتصالات**: وتشمل شبكات الاتصال التي تربط الأجهزة التقنية ببعضها، محليا ونطاقيا ودوليا، وتتيح فرصة اختراق النظم عبرها، و هي بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي.
- **المورد البشري**: ومحور الخطر هو الإنسان، سواء المستخدم أم الشخص المناط به مهام تقنية معينة تتصل بالنظام، فإدراك هذا الشخص حدود صلاحياته، وإدراكه آليات التعامل مع الخطر، وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية، هي مسائل رئيسة يعنى بها نظام الأمن الشامل، وتحديدا في بيئة العمل المرتكزة على نظم الكمبيوتر، وقواعد البيانات. وهذا موضح في الشكل الثاني.

الشكل الثاني: مواطن الاعتداء

المصدر: من إعداد الباحثة.

المطلب الرابع: الأخطار والحماية منها.

تعاني المنظمة في ظل استخدامها الواسع لتكنولوجيا المعلومات بجملة من الأخطار التي تتعرض لها، وبالتالي تتطلب من إدارة نظم المعلومات كثيرا من الوقت والجهد والموارد المالية لعملية الحماية منها. سنتناول الآن الأخطار التي تواجه العمليات الالكترونية، وكيفية الحماية منها. [5]

أولا: الأخطار التي يمكن أن تتعرض لها العمليات الالكترونية

يمكن تصنيف الأخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات الى ثلاث فئات:

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 المنظمات.

ب . الأخطار البيئية Environmental Hazard

وهذه تشمل الزلازل والعواصف والفيضانات والأعاصير، والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق، إضافة إلى المشاكل القائمة في تعطل أنظمة التكييف والتبريد وغيرها، وتؤدي هذه الأخطار إلى تعطل عمل هذه التجهيزات وتوقفها لفترات طويلة نسبيا، لإجراء الإصلاحات اللازمة، واسترداد البرمجيات وقواعد البيانات.

ج. الجرائم المحوسبة Computer Crime

تمثل هذه تحديا كبيرا لإدارة نظم المعلومات، لما تسببه من خسارة كبيرة، وبشكل عام يتم التمييز بين ثلاثة مستويات للجرائم المحوسبة، وهي:

1. **سوء استخدام جهاز الحاسوب:** وهو الاستخدام المقصود الذي يمكن أن يسبب خسارة للمنظمة، أو تخريبا لأجهزتها بشكل منظم.
2. **الجريمة المحوسبة:** وهي عبارة عن سوء استخدام أجهزة الحاسوب بشكل غير قانوني، يؤدي إلى ارتكاب جريمة يعاقب عليها القانون الخاص بجرائم الحاسوب.
3. **الجرائم المتعلقة بالحواسيب:** وهي الجرائم التي تستخدم فيها الحواسيب كأداة لتنفيذ الجريمة.

ويمكن أن ترتكب الجرائم المحوسبة سواء من قبل أشخاص خارج المنظمة، يقومون باختراق نظام الحاسوب (غالبا من خلال الشبكات) أو من قبل أشخاص داخل المنظمة، يملكون صلاحيات الدخول إلى النظام ولكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة. وتشير الدراسات التي أجرتها دائرة المحاسبة العامة وشركة (Orkand) للاستشارات 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، وأن جرائم الحاسوب تزداد بصورة واضحة؛ مما جعلها تشكل تحديا خطيرا يواجه الإدارات العليا عموما، وإدارة نظم المعلومات على وجه الخصوص.

ثانيا: الحماية من الأخطار

تعتبر عملية الحماية من الأخطار التي تهدد الشبكة المعلوماتية من المهام المعقدة والصعبة، والتي تتطلب من إدارة نظم المعلومات كثيرا من الوقت والجهد والموارد المالية؛ وذلك للأسباب التالية:

أ. العدد الكبير من الأخطار التي تهدد عمل الشبكة.

ب. توزع الموارد المحوسبة على عديد من المواقع التي يمكن أن تكون أيضا متباعدة.

ج. وجود التجهيزات المحوسبة في عهدة أفراد عديدين في المنظمة، وأحيانا خارجها.

د. صعوبة الحماية من الأخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية.

هـ. التقدم التقني السريع يجعل كثيرا من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها.

و. التأخر في اكتشاف الجرائم المحوسبة؛ مما لا يتيح للمنظمة إمكانية التعلم من التجربة والخبرة المتاحة.

ز. تكاليف الحماية يمكن أن تكون عالية؛ بحيث لا تستطيع عديد من المنظمات تحملها.

هذا، وتقع مسؤولية وضع خطة الحماية للأنشطة الرئيسة على مدير الشبكة في المنظمة، على أن تتضمن هذه الخطة إدخال وسائل الرقابة التي تضمن تحقيق ما يلي:

- الوقاية من الأخطار غير المتعمدة؛
- 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.

المبحث الثاني: ماهية إستراتيجية أمن المعلومات.

إن إستراتيجية أمن المعلومات هي مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنظمة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها.

سنتناول الآن مفهوم وأهداف إستراتيجية أمن المعلومات، وخصائصها ومميزاتها، ومنطلقاتها، وفي الأخير مكوناتها وخطواتها.

المطلب الأول: مفهوم وأهداف إستراتيجية أمن المعلومات

سنتطرق في هذا المطلب إلى مفهوم وأهداف استراتيجية أمن المعلومات

أولا–مفهوم استراتيجية أمن المعلومات: تعرف بأنها "مجموعة القواعد التي تتعلق بالوصول إلى المعلومات، والتصرف فيها، ونقلها داخل هيكل يعتمد المعلومة عنصرا أساسيا في تحسين أدائه، وبلوغ أهدافه."[6]

كما تعرف أيضا على أنها "مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة، وتتصل بشؤون الدخول الى المعلومات والعمل على نظمها وإدارتها."[7]

كما أنها "الخطة التي تعرف الاستعمال المقبول لجميع الوسائط الإلكترونية في شركة أو منظمة."[8]

و كذلك هي «مجموعة من القوانين المنظمة لكل الأنشطة ذات الصلة في موقع ما، وهذه السياسة تصدرها جهة مسؤولة، تقر بمسؤوليتها تجاه أمن وحماية معلومات المنشأة من جميع مصادر التهديد".[9]

إستراتيجية أمن المعلومات هي "مجموعة قوانين أمنية تسيطر على نظام المعلومات، وتزوده بمستوى حماية موثوق به. وهذه السياسات يجب أن تُوجه الإدارة وسبل الحماية، والمصادر المرتبطة بالمعلومات وبنظام المعلومات. إن مستوى قسوة تلك السياسات عادة مرتبط بمستوى المخاطر المراد تجنبها".[10]

إذن إستراتيجية أمن المعلومات هي الخطة التي تعرف الاستخدام المقبول أو المرضي لجميع الوسائط الالكترونية في المنظمة. هناك عناصر أساسية يجب أخذها بالاعتبار عند تنظيم وتطوير إستراتيجية أمنية، فما هي البيانات التي تحتاج إلى حماية؟ ولماذا؟ وما هي الآثار المالية السلبية إذا حدث اختراق أو إذا فقدت الثروة المعلوماتية أو حطمت؟ ومن المهم جداً مراجعة كل المفاهيم الرئيسة عند تطوير أي سياسة أمن معلومات. وفيما يلي ثلاثة مفاهيم رئيسة، وهي: القابلية للتطبيق، توفر القوة البشرية المدربة، الدعم القانوني والإداري، وضوح المسؤوليات، تحديد مسؤوليات المستخدمين والمديرين والعملاء، الإلزامية في التطبيق، دعم الإدارة والإدارة القانونية.

ولكي تكون هذه الاستراتيجية فعالة وهادفة فلا بد أن:

* يساهم في إعدادها وتفهمها وتقبلها وتنفيذها مختلف مستويات الوظيفة في المنظمة الواحدة؛

* وأن تلبي حاجتها إلى التعاون والدعم الكامل من كافة مستويات المؤسسة.

ومن هنا يتضح أن المعنيين بإعداد سياسة أمن المعلومات يتوزعون إلى مراتب وجهات عديدة داخل المنظمة، تشمل:

- مسؤولي أمن الموقع؛
- ومديري الشبكات؛
- وموظفي وحدة الكمبيوتر؛
- ومديري الوحدات المختلفة؛
- ومستويات الإدارة العليا؛
- إلى جانب الإدارة القانونية.

ثانيا: أهداف استراتيجية أمن المعلومات: تتمثل أهداف الاستراتيجية الأمنية في:

1. ترجمة وتوضيح الأمن كما تم تعريفه في القواعد والمبادئ والأهداف العليا للمنظمة.
2. تعريف المستخدمين بمسؤولياتهم وواجباتهم تجاه أمن نظم المعلومات، والذي يتضمن الأفراد، الأجهزة، البرامج، المعلومات...الخ.
3. بيان الإجراءات التي يجب اتباعها لتفادي المخاطر والمهددات، والتعامل معها إذا ما وقعت.
4. تحديد الآليات التي يتم من خلالها تنفيذ وتحقيق المسؤوليات والواجبات لكل مستخدم.

المطلب الثاني: خصائص ومميزات إستراتيجية أمن المعلومات

سنتناول الآن مميزات وخصائص إستراتيجية أمن المعلومات.

أولا: خصائص ومميزات إستراتيجية أمن المعلومات

من مميزات إستراتيجية أمن المعلومات ما يلي:

- يجب أن تكون مناسبة اقتصاديا (ذات جدوى اقتصادية)؛
- يجب أن تكون مفهومة للمستخدمين؛
- يجب أن تكون واقعية تتناسب مع واقع المنظمة؛
- يجب أن تكون متناغمة مع أهداف المنظمة؛
- يجب أن تكون مرنة وقابلة للمعالجة؛
- يجب أن توفر حماية معقولة لأهداف الإدارة المعلنة؛
- يجب أن تكون مستقلة، (لا تعتمد على أجهزة Hardware ولا برامج Software محددة).

ثانيا: خصائص سياسة الأمن الجيدة

و تتمثل خصائص سياسة الأمن الجيدة في أنها:

- يجب أن تكون قابلة للتطبيق، من خلال الإجراءات والتوجيهات الإدارية؛
- يجب تحديد المسؤوليات على كل مستويات الهيكل التنظيمي؛
- يجب أن تكون موزعة على كل وحدات المنظمة؛
- يجب أن تكون موثقة (للمرجعية)؛
- يجب أن تكون مرنة وفعالة لأطول فترة ممكنة.

المطلب الثالث: منطلقات إستراتيجية أمن المعلومات

إن البحث في السياسات، وتوفير الوسائل التقنية والإجراءات الضرورية لحماية المعلومات، تستوجب طرح تساؤلات من شأنها أن تسمح بتحديد منطلقات خطة واضحة المعالم تعد وتعتمد وجوبا لضمان أمن المعلومات. و من أهم هذه التساؤلات:[11]

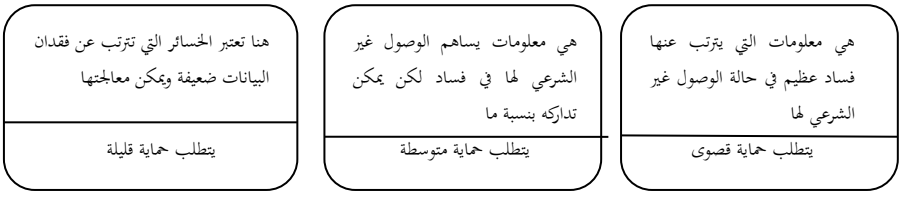
هل تتطلب كل المعلومات نفس القدر من الحماية؟ وما الذي نريد أن نحميه؟

ما هي المخاطر التي يمكن أن تهدد المعلومات فتستوجب الحماية؟

ما هي وسائل هذه الحماية؟ كيف نتصرف في حالة تحقق خطر على الرغم من توفر هذه الوسائل؟ هل تتطلب كل المعلومات نفس القدر من الحماية؟ وما الذي نريد أن نحميه؟

تصنيف المعلومات: يتم بناء على درجة المخاطر المترتبة على اختراق المعلومات من قبل الأشخاص:

الشكل الثالث: تصنيف المعلومات



Source : David Jarmon, op.cit. , 2002, p 1

تصنيف المعلومات

- يتطلب حماية قصوى: هي المعلومات التي يترتب فساد عظيم في حالة الوصول غير شرعي لها؛
- يتطلب حماية متوسطة: هي معلومات يساهم الوصول غير شرعي لها في فساد يمكن تداركه بنسبة ما؛

- يتطلب حماية قليلة: هنا تعتبر الخسائر التي تترتب عن فقدان البيانات ضعيفة ويمكن معالجتها.

وما هي المخاطر التي يمكن أن تهدد المعلومات؛ فتستوجب الحماية؟

- **تحديد المخاطر**

يجب تحديد المخاطر التي قد تهدد نظم المعلومات، بدءا بالمشاكل العادية مثل قطع التيار الكهربائي عن الأجهزة، إلى مخاطر اختراق تلك النظم من الخارج، مرورا بخلل في صيانة التجهيزات والبرمجيات، أو سوء استخدام الموظفين لوسائل الحماية مثل كلمات العبور.

وما هي وسائل الأمن؟

ينبغي أن تُعد كل مؤسسة طريقتها الخاصة لتوفير أمن معلوماتها من المخاطر في حدود إمكاناتها التنظيمية والميزانية المرصودة للحماية، وينبغي أن لا تكون إجراءات الأمن ضعيفة بحيث لا تضمن الحماية المطلوبة، ولا تكون مبالغا فيها إلى حد يؤثر في طبيعة أداء خدمات نظام المعلومات.

كيف نتصرف في حالة تحقق خطر على الرغم من توفر هذه الوسائل ؟

***كيفية مواجهة المخاطر عند حصولها**

وعلى الرغم مما يؤخذ من احتياطات لازمة لتأمين بعض المخاطر يظل حصولها واردا، وفي إطار سياسة أمن المعلومات، ينبغي التفكير في إعداد خطة تبين في مرحلتها الأولى الإجراءات التقنية والقانونية للحد من الخسائر، وتأمين استمرارية العمل بطرق ووسائل بديلة.

ثم تبين هذه الخطة، في المرحلة الثانية، إجراءات التحليل لطبيعة المخاطر الحاصلة ودواعي حصولها.

وعلى أساس ذلك تحدد إجراءات إصلاح ما أُفسد، والعودة إلى وضعية ما قبل حصول الخطر، وضمان منع حصوله لاحقا. [12]

المطلب الرابع: مكونات وخطوات إستراتيجية أمن المعلومات

تتكون إستراتيجية أمن المعلومات من ثلاثة مكونات هي:

1. **الإستراتيجية** نفسها، والتي توثق لدوافع حماية المؤسسة لبياناتها، وما هي هذه البيانات، والتي يمكن بناؤها في الخطوات التالية:[13]

- تحديد المادة (Subject) (الموضوع) محل الاهتمام، والمراد عمل إستراتيجية له؛
- ماهي العمليات والنشاطات المسموح بها، وما هي المرفوضة(غير المسموح بها)، ولمن من المستخدمين؟

- تحديد الأشخاص (المستخدمين) المتأثرين بهذه الإستراتيجية؛
- تحديد كيفية تطبيق الإستراتيجية في بيئة المنظمة؛
- تحديد المخاطر المتوقعة في البيئة المحددة؛
- تحديد وتصنيف البيانات وموارد النظام؛
- تحديد خدمات الأمن الأساسية في بيئة المنظمة؛
- تحديد قائمة السياسات التي أُنشئت؛
- إنشاء تحليل لانسياب البيانات المصنفة منذ مرحلة الإنشاء وحتى الحذف من النظام؛
- توثيق الإستراتيجية.

2. **المعايير (Standard)** وهي توثق لماهية المقاصد المنشودة لتطبيق وإدارة أمن المعلومات في المنظمة.

3. **الإجراءات (Procedures)** وهي توثق للكيفية التي تنجز بها المنظمة المتطلبات المفروضة بالمعايير والإستراتيجيات، وهي الأدوات التي بها تُحول السياسات إلى أحداث وعمليات.

بعد إنشاء السياسات يجب توزيعها على كل مستويات الهيكل التنظيمي (مستخدمين، موظفين، الإدارة، الزبائن، الاستشاريين...الخ).

لضمان صلاحية السياسات يجب تعهدها بالمراجعة المستمرة، وذلك بتحديث آلياتها وأدواتها، ويجب عكس التغييرات في بيئة عمل المنظمة على سياسات التأمين أولا بأول.

الخاتمة:

ناقشت الدراسة أهم جوانب إستراتيجية أمن المعلومات، ولقد توصلت إلى ما يلي:

-إن أمن المعلومات هو ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزونة في أجهزة الحاسوب، إضافة إلى الأجهزة الملحقة، وشبكات الاتصالات، والتصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزونة، أو تلك التي ترمي إلى نقل أو تغيير أو تخريب التخزين المعلوماتي لهذه القواعد.

- تواجه المنظمات مخاطر أمنية من مصادر كثيرة، منها الأخطاء البشرية، الأخطار البيئية، وأخيرا الجرائم المحوسبة؛ ولذلك يجب وضع إستراتيجية أمنية فعالة لمواجهتها.

– إن الهدف من صياغة إستراتيجية الأمن وتنفيذها هو تحسين توافر المعلومات وتكاملها، وخصوصيتها داخل وخارج المنظمة.

– عند بناء إستراتيجية أمنية يجب تحديد الإجابة عن التساؤلات الثلاثة الرئيسة: ماذا أريد أن أحمي؟ من ماذا أحمي المعلومات؟ كيف أحمي المعلومات؟

– في عملية تقدير المخاطر، يجب التأكد من ترتيب المخاطر حسب شدة خطورتها و أولويتها؛ وهذا سيساعد في اتخاذ القرار، وتقليل الإنفاق في حماية أشياء لا تستحق ذلك.

– إن الاستراتيجية الأمنية تتطلب من المنظمة اتباعها، والقيام بمراجعتها بشكل دوري؛ للتأكد من ملاءمتها للتغيرات والشروط المتغيرة.

– إن أمن المعلومات يحتاج إلى إستراتيجية قوية؛ بهدف حماية البنية التحتية والتصدي للتهديدات.

وعليه يمكن حصر التوصيات في النقاط الآتية:

_ العمل على حماية المعلومات عند تخزينها، وذلك بتشفيرها، أو وضع كلمة مرور خاصة عند الحفظ والتخزين على مختلف الوسائط؛ حتى لا يتمكن أحد من اختراقها.

–أهمية التوعية ونشر ثقافة أمن المعلومات بين جميع الموظفين تتلخص في الآتي:

1–إنشاء دائرة خاصة بأمن المعلومات تزود بإطارات مؤهلة لإدارتها، ومنحها صلاحيات قوية تؤهلها لتطوير وتطبيق السياسات الأمنية، وذلك بدعم الإدارة العليا لها.

2– رفع الوعي الأمني لدى جميع موظفي المنظمة على اختلاف مستوياتهم، وذلك بعمل دورات تدريبية خاصة بهم.

3–إضافة ميزة إغلاق رقم المستخدم بعد ثلاث محاولات فاشلة؛ وذلك لمنع محاولة الدخول على النظام بتخمين كلمة السر.

4– لتطبيق سياسة صارمة تجاه كلمة السر يجب وضع مواصفات قياسية لكلمة السر، من حيث عدد الحروف وتنوعها بين الحروف والأرقام والرموز، وعدم تكرار الحروف، وعدم إعادة استخدام الكلمة نفسها حتى انقضاء فترة من الزمن، وليكن عاماً مثلا، وطلب تغيير الكلمة بصورة دورية، وتضمين هذه المواصفات في البرامج التطبيقية لفرض السياسة على جميع المستخدمين.

5–بما أن معظم الأعطال ناتجة عن إصابة الأنظمة بالفيروسات؛ فعلى المنظمة وضع إستراتيجية شاملة لمكافحة الفيروسات، وذلك بجلب وتركيب برامج المكافحة المعروفة والمشهود لها بفاعليتها، بحيث تشمل الإستراتجية تركيب برامج مراقبة واكتشاف الفيروسات، وبتوفيق البرامج بالخوادم، بحيث لا تسمح للأجهزة الطرفية بالدخول إليها إذا لم تكن بها برامج اكتشاف الفيروسات حديثة ومتلائمة

مع الخادم، من برامج الحماية، كما يجب أن تتضمن الإستراتيجية عدم نقل أو جلب البرامج والبيانات لنظم المنظمة بأي وسيلة، ما لم يتم فحصها وتوثيقها من الجهة المختصة بالمنظمة والتأكد من خلوه من الفيروسات.

6-قيام المنظمة بفرض الإطار العام للسياسات الأمنية لحماية نظم معلوماتها، وذلك بالمتابعة والتفتيش المستمر للتأكد من التزام المنظمة بتطبيق السياسات بدقة.

الهوامش

[1] ابراهيم سلطان، نظم المعلومات الإدارية (مدخل إداري)، الدار الجامعية، 2000، ص41.

[2] سونيا محمد البكري، نظم المعلومات الإدارية (المفاهيم الأساسية)، الدار الجامعية، القاهرة، 2000، ص98.

[3] – علوطي لمين، أثر تكنولوجيا المعلومات والاتصال على إدارة الموارد البشرية في المؤسسة، مجلة علوم إنسانية، السنة السادسة، العدد 38، صيف 2008، ص21.

[4] – (نجم عبد الله الحميدي، نظم المعلومات الإدارية (مدخل معاصر)، الطبعة الأولى، دار وائل للنشر، عمان، الأردن 2005، ص 265).

[5] http://www.ao-academy.org/docs/45D0~1.DOC, consultée à 12/12/2014.

[6] –سياسة أمن المعلومات

http://www.google.ps/url?sa=t&rct=j&q=%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9+%D8%A7%D9%85%D9%86+%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA+DOc&source=web&cd=20&ved=0CFoQFjAJOAo&url=http%3A%2F%2Fsana1111.files.wordpress.com%2F2011%2F03%2Fd8b3d98ad8a7d8b3d987-d8a7d985d986-d8a7d984d985d8b9d984d988d985d8a7d8aa-information-security-policy.doc&ei=1-HzTrrIFtS18QOo6qm5AQ&usg=AFQjCNGwOA0boLfpievIw0XS0wDkmz-hgg&cad=rja). بتاريخ 30/ 10/ 2014.

[7] – (عائض المري، أمن المعلومات، ماهيتها وعناصرها واستراتيجياتها، معلومات قانونية، الدراسات والاستشارات القانونية، 6 نوفمبر2001، انظر الموقع الإلكتروني:
http://www.dralmarri.com/show.asp?field=res_a&id=205، بتاريخ 2014/11/12.

[8] – (سلمان بن علي بن وهف القحطاني، أمن المعلومات (أمن المعلومات في ضوء التطور التقني والمعلوماتي الحديث في الشبكات اللاسلكية النقالة)، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي – الإمارات العربية المتحدة، 2003/4/26، ص 13).

[9]- The CISSP All-in-one Certification Exam Guide, By Shon Harris, 2002, Page 93

[10]- Kevin M. Dulany , Security, It's Not Just Technical " , GSEC Practical Assignment , v1.3 , 15 January 2002 , SANS Institute 2002 , p 4 .

[11] (David Jarmon , "A Preparation Guide to Information Security Policies" , SANS Security Essentials GSEC Practical Assignment , Version 1.3, SANS Institute 2002, pp 1-3, 11-14

[12] موقع عبد المجيد ميلاد في تكنولوجيا المعلومات والاتصال.
http://www.abdelmajid-miled.com/articles_ar1.php?id=16)، بتاريخ 2014/11/12.

[13] " Enterprise Information Security Policies", Georgia Technology Authority , September 10, 2002 , pp 10-11.
URL:http://gta.georgia.gov/vgn/images/portal/cit_1210/62/58/1218035EnterpriseInforSecurityPoliciesGEITLF.pdf), consultée à 30/10/2014.

المراجع:

1- البكري سونيا محمد ، نظم المعلومات الإدارية (المفاهيم الأساسية)، الدار الجامعية، القاهرة، 2000.

2- الحميدي نجم عبد الله، نظم المعلومات الإدارية (مدخل معاصر)، الطبعة الأولى، دار وائل للنشر، عمان، الأردن، 2005.

3- سلطان إبراهيم، نظم المعلومات الإدارية (مدخل إداري)، الدار الجامعية، 2000.

4- سياسة أمن المعلومات
http://www.google.ps/url?sa=t&rct=j&q=%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9+%D8%A7%D9%85%D9%86+%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA+DOc&source=web&cd=20&ved=0CFoQFjAJOAo&url=http%3A%2F%2Fsana1111.files.wordpress.com%2F2011%2F03%2Fd8b3d98ad8a7d8b3d987-d8a7d985d986-d8a7d984d985d8b9d984d988d985d8a7d8aa-information-security-policy.doc&ei=1HzTrrIFtS18QOo6qm5AQ&usg=AFQjCNGwOA0boLfpievIw0XS0wDkmz-hgg&cad=rja، بتاريخ 30/ 2014/10.

5- علوطي لمين، أثر تكنولوجيا المعلومات والاتصال على إدارة الموارد البشرية في المؤسسة، مجلة علوم إنسانية، السنة السادسة، العدد 38، صيف 2008.

6- القحطاني سلمان بن علي بن وهف، أمن المعلومات (أمن المعلومات في ضوء التطور التقني والمعلوماتي الحديث في الشبكات اللاسلكية النقالة)، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي – الإمارات العربية المتحدة، 26 /2003/4.

7- المري عائض، أمن المعلومات، ماهيتها وعناصرها وإستراتيجياتها، معلومات قانونية، الدراسات والاستشارات القانونية، 6 نوفمبر2001، انظر الموقع الالكتروني:

http://www.dralmarri.com/show.asp?field=res_a&id=205، بتاريخ 2014/11/12.

8- موقع عبد المجيد ميلاد في تكنولوجيا المعلومات والاتصال: http://www.abdelmajid-miled.com/articles_ar1.php?id=16، بتاريخ 2014/11/12.

Les ouvrages :

1- Dulany Kevin M., "Security, It's Not Just Technical», GSEC Practical Assignment , v1.3 , 15 January 2002 , SANS Institute 2002.
2- Enterprise Information Security Policies», Georgia Technology Authority, September 10, 2002, pp 10-11. URL:http://gta.georgia.gov/vgn/images/portal/cit_1210/62/58/1218035EnterpriseInforSecurityPoliciesGEITLF.pdf., consultée à 30/10/2014.
3- http://www.ao-academy.org/docs/45D0~1.DOC, consultée à 12/12/2014.
4- Jarmon David, "A Preparation Guide to Information Security Policies" , SANS Security Essentials GSEC Practical Assignment , Version 1.3 , SANS Institute 2002.
5- The CISSP All-in-one Certification Exam Guide, By Shon Harris, Published by Mcgraw-Hill/Osborne 2600 Tenth Street, Berkely, California 94710, U.S.A. 2002.