المحاضرة الثـــامـــــنــة

حماية وأمن المعلومات

يرتبط موضوع الأمن ارتباطا وثيقا بالمعلومة في المنظمة، اذ ان نوع المعلومات وكميتها وطريقة استغلالها تعتبر الأساس في نجاح عملية اتخاذ وصنع القرارات داخل المؤسسات المعاصرة وعليه فإن للمعلومة قيمة عالية تستوجب وضع الضوابط الازمة لاستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، وعليه ان توفير الحماية اللازمة للمعلومات من بين الأساسيات ومن بين الأنشطة الهامة ومن مهام ومسؤوليات الإدارة، فحسب هنري فايول في كتابه الإدارة العامة والصناعية 1916 الأمن هو حماية الأفراد والممتلكات بما فيها من أصول ومعلومات وتقارير خاصة بالمؤسسة.

فامن المعلومات من نظم التحكم الداخلية بما تقوم به من رقابة وتدقيق للأعمال المتعلقة بنظم المعلومات وهي تتعدى الضوابط والإجراءات التقنية.

1 مفهوم أمن المعلومات

يرتبط مفهوم الأمن المعلوماتي بصفة مباشرة مع أمن الحواسيب وذلك في سياق عالمي يتميز باختراق منظمات الحواسيب وتخريب المعلومات، وعليه فمن الضروري التفكير في الإجراءات الدفاعية والوقائية لحماية أمن المعلومات مما أصبح من مسؤوليات إدارة المنظمات على تحمل مسؤوليات ضمان امن المعلومات والحفاظ عليها.

فمجال أمن المعلومات يعنى بحماية المعلومات من الاختراق، والوصول واستعمال المعلومات بغير حق، وحتى التجسس والاطلاع عليها من قبل المتطفلين، وإتلافها وتدميرها وتعديلها، وهو يشكل احدى المجالات التي لا تتفرع علم الحاسوب، والذي يرتبط بدوره بمجالات أمن الانترنت وأمن الشبكات ويحوز على ثلاثة أبعد أساسية:

البعد الأكاديمي والذي يهتم بالبحث في نظريات واستراتيجيات توفير الحماية للمعلومة من المخاطر التي تهددها ومنع الوصول إليها وهدرها من غير ذوي الصالحية، وحمايتها من أي تهديد خارجي، ويشمل هذا المصطلح الطرق والوسائل والإجراءات اللازمة والواجب توفيرها لتحقيق الحماية من المخاطر التي قد تواجهها من الداخل والخارج

البعد التقني: والذي يركز على البحث في الوسائل والأدوات الخاصة لضمان حماية المعلومات على السياق الداخلي والخارجي للمؤسسة والبحث عن أفضل السبل لتأمينها

البعد القانوني: والتي تعنى بالتدابير والإجراءات القانونية اللازمة لحماية أمن المعلومات والبحث في التشريعات والاطر القانونية لتحديد المسؤوليات والأنشطة غير المشروعة ومعاقبة مرتكبي الاعتداء بغرض توفير الردع.

كما يعرف الأمن المعلوماتي على أنه مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات.

ويرتكز أمن المعلومات على الحفاظ على أمن المعلومات من مخاطر التلف، الضياع أو من مخاطر الاستخدام غير الصحيح بمعنى أخر إبقاء المعلومات تحت السيطرة المباشرة والكاملة ووضع خطط لتخزين نسخ إضافية من البيانات والبرمجيات.

ويرى كل من Whitman & Mattord 2011 [44] بأن أمن المعلومات هو الحفاظ على سرية وتوفر وسلامة المعلومات في مراحل المعالجة والحفظ والنقل، ويتحقق ذلك عبر التطبيق الفعلي للسياسات الأمنية ومن خلال تعزيز الوعي والتعلم والتدريب.

ويرى الباحثان بأن المؤسسات التي تهدف لتحقيق إدارة أمن نظم المعلومات عليها التحكم في أمن معلومات كل من المجالات التالية:

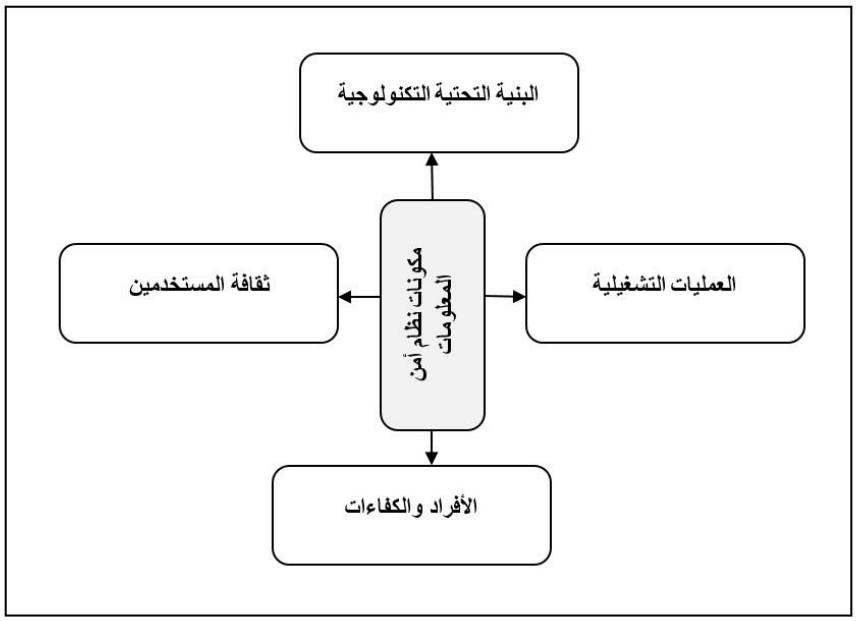
- ✓ الأمن المادي: بما يشمله من مصادر وممتلكات ومباني لمنع الوصول اليها.
- ✓ أمن الأفراد: لحماية الأفراد والمجموعات الذين لهم حق الوصول للمعلومات.
- ✓ أمن الاتصالات: لحماية الوسائط والتكنولوجيا المستخدمة والمحتوى.
- ✓ امن الشبكات لحماية مكونات الشبكة والتراسل والمحتويات.
- ✓ أمن البيانات: لحماية سرية وسلامة وتوافر المعلومات.

على العموم يعرف أمن نظم المعلومات بأنها: العمليات والتدابير والتوجيهات التي تصدرها إدارة المؤسسة بهدف حماية مواردها التقنية وما تحتويه من معلومات في مختلف أشكالها بغرض تحقيق سالمتها وتوافرها وسريتها وفق الصلاحيات والترتيبات المتعارف عليها.

2 مكونات أمن نظم المعلومات :

تتكون بيئة نظام أمن نظم المعلومات من أربع مكونات أساسية وهي :

[44] Whitman Michael, Mattod Herberet(2011)Principles of Information Security, 4 th edition, Boston : Cengage Learning /Course Technology.



- التكنولوجيا
- العمليات
- الأفراد
- الثقافة

شكل بياني رقم 14 يوضح أبعاد نظام أمن المعلومات

وتعتبر هذه المكونات أساسية بحيث لا يمكن تحقيق الأمن بدون توافر مجموعة من العوامل التي تخص كل من السرية وذلك بإتاحة البيانات فقط لأصحابها، التكاملية والسلامة وذلك بحماية البيانات من عمليات الحذف والتخريب وفي الأخير التوفر والاتاحة من خلال تأمين استمرارية وصول المستخدمين الى المعلومات الخاصة بهم كما يأمن لهم سهولة الاستخدام.

3 أهمية أمن المعلومات:

تتمثل أهمية أمن الملومات فيما يلي[45] :

- ✓ اعتماد القطاعات الاقتصادية والعمومية والصحية عل صحة ودقة الملومات لتنفيذ أنشطتها؛

[45] Dagorn, N. , Politiques en matière de sécurité des systèmes d'information inter-organisationnels: une enquête dans dix grandes entreprises. *Systèmes d'information et management, 13*(2), 2008, 97-125.

- ✓ حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق، تغطي المخاطر التي يمك أن تنبثق من خلال التعامل مع الأطراف الأخرى؛
- ✓ التحول الرقمي المتسارع لإنشاء بيئة لكرتونية آمنة تخدم مختلف القطاعات؛
- ✓ النمو السريع في استخدام التطبيقات الالكترونية المرتبطة بشبكة الانترنت، والتي تتطلب بيئة آمنة؛
- ✓ الحاجة الى حماية البنية التحتية للشبكات المعلوماتية، من أجل استمرارية مختلف الاعمال لجميع القطاعات؛
- ✓ تزايد التهديدات الخاصة بالإجرام الالكتروني وظهور الحروب السيبرانية كشكل جديد من الحروب التي تهدد أمن واستقرار الحكومات.

4 الأخطار التي يمكن أن تتعرض لها أنظمة المعلومات:

ان اختراق أنظمة المعلومات ونظم الشبكات والمواقع المعلوماتية خطرا يقلق العديد من المؤسسات في السنوات الأخيرة، ولذلك يعد تحديد طبيعة الأخطار التي تتعرض لها أنظمة معلوماتها والتي يمكن أن تكون مقصودة كسرقة المعلومات أو ادخال الفيروسات وغيرها والتي قد يكون مصدرها من داخل المؤسسة أو من خارجها، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية والكوارث الطبيعية ويمكن أن تكون لها عدة مصادر:

- ✓ **الأخطاء البشرية:**

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.

- ✓ **الأخطار البيئية:**

وتشمل الزلازل والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق...الخ، وتؤدي هذه الأخطار إلى تعطل عمل التجهيزات وتوقفها لفترة طويلة نسبيا لاسترداد البرمجيات وقواعد البيانات .

- ✓ **الجرائم المحوسبة:**

تمثل هذه الجرائم تحديا كبيرا لما تسببه من خسارة كبيرة، ويمكن أن تتم هذه الجرائم من قبل أشخاص خارج المنظمة يقومون باختراق الأنظمة غالبا من خلال الشبكات أو من قبل أشخاص داخل المنظمة يملكون صلاحيات الدخول إلى النظام ولكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة.

5 استراتيجية أمن المعلومات:

تتمثل أهداف الاستراتيجية الأمنية فيما يلي[46]:

- ✓ توضيح المعالم الأمنية والقواعد الواجب اتباعها لتحقيق الأهداف العليا للمؤسسة؛
- ✓ توضيح مسؤوليات المستخدمين وواجباتهم اتجاه امن نظم المعلومات والذي يتضمن الأفراد الأجهزة والبرامج؛
- ✓ تحديد الإجراءات اللازم اتباعها لتفادي المخاطر والتهديدات الأمنية وكيفية التعامل معها في حين حدوثها؛

[46] Barlette, Y., Une étude des comportements liés à la sécurité des systèmes d'information en PME. Systèmes d'information et management, 13(4), 2008, 7-30.

- ✓ تحديد الآليات التي يتم من خلالها تنفيذ وتحقي المسؤوليات والواجبات لكل مستخدمي الأنظمة المعلوماتية.

1.5 الإجراءات الخاصة لحماية أمن نظم المعلومات

بعد استعراض اهم المخاطر التي تواجه نظم المعلومات وتحول دون حماية المعلومات في داخلها، تظهر سبل حماية النظم من خلال تفعيل العوامل التالية:

- ✓ **برامج مكافحة الفيروسات**

هي البرامج المصممة لاتخاذ جميع الاحتياطات اللازمة لحماية الحواسيب من الفيروسات، وتعتبر من أهم وسائل الحماية حيث تقوم بمنع القضاء عليها فضلا عن قيامها بتحديث نفسها بشكل آلي عن طريق ارتباطها بشبكة الانترنت لتزيد من كفاءتها وقدرتها على مكافحة الفيروسات الجديدة. غير نه يجب على المستخدمين للحواسيب تحديث البرامج وتنويعها لمكافحة الفيروسات بصفة دورية ومستمرة لكي تتمكن من التعرف عليها والقضاء عليها.

- ✓ **كلمات المرور**

هي بمثابة جواز مرور المستخدم الى الشبكة، فكلمة المرور تثبت للشبكة بأنك أنت الشخص المخول للدخول اليها، وهي أبسط أنواع حماية المعلومات على شبكة الانترنت، فهي تعمل على حماية المعلومات الشخصية وغيرها من البيانات وحماية لبعض الأنشطة الرقمية كالدفع الالكتروني. ونظرا لأهميتها توجب علينا ان نحرص عليها ويكون بمراعاة بعض الشروط:

- ✓ اختيار كلمة مرور صعبة ولا يسهل تخمينها،
- ✓ عدم اطلاع الغير عليها،

- ✓ تغييرها بشكل دوري،
- ✓ عدم الاعتماد على كلمة واحدة والاعتماد على مزيج من الحروف والأرقام حتى تصعب قرصنتها،
- ✓ عدم تضمنها لبيانات شخصية كاسم المستخدم او تاريخ ميلاده،
- ✓ ان لا تقل عن عشرة حروف او ارقام.

- ✓ **جدران الحماية**

يكون جدار الحماية الناري اما برنامجا او جهازا لحماية الشبكة والخادم من المتسللين وتختلف الحماية حسب احتياجات المستخدم، فاذا استدعت الحاجة الى وضع جدار حماية على عقدة منفردة عاملة على شبكة واحدة فان جدار الحماية الشخصي هو الخيار المناسب وفي حالة وجود حركة مرور داخلة وخارجة من عدد من الشبكات، فيتم استخدام مصافي لجدار الحماية في الشبكة لتصفية جميع الحركة المرورية علما بان الكثير من الشبكات والخوادم تاتي مع نظام جدار حماية افتراضي. أحيانا تقوم شبكات المعلومات بوضع جدار الحمية لعزل شبكاتها عن شبكة الانترنت ولا يكون هذا العزل كليا حتى يتمكن المستخدمين من الاستفادة من بعض خدمات الانترنت ومنع المخربين من الولوج الى الشبكة الداخلية واختراق المعلومات.

- ✓ **التحديث التلقائي**

يعد التحديث التلقائي والدائم من بين أهم نقاط الحماية للشبكات وذلك لسد نقاط الضعف في البرامج والأنظمة، ونظرا لصعوبة مطالبة الشركات لمستخدمي هذه البرامج بتحديث البرامج بأنفسهم فان معظم الشركات المصنعة لهذه البرامج تعمل على خاصية التحديث الآلي والتلقائي

لهذه البرامج كي تعمل بالاتصال التلقائي على فترات مينة والبحث عن التحديثات الجديدة وتنزيليها تلقائيا.

- ✓ **التشفير**

بتم من خلال ادخال تعديلات على المعلومات عند ارسالها الى جهة معينة او تحويليها الى رموز غير ذات معنى، حيث عند وصولها للأشخاص لا يستطيعون فهمها او الاستفادة منها لذا فهي عبارة عن تشفير وتحويا للنصوص العادية الواضحة الى نصوص مشفرة وغير مفهومة.

التخزين الاحتياطي

ويكون ذلك اما بالاعتماد على نسخ المعلومات وحفظها في أماكن أمنة بحيث يمكن الرجوع اليها في حالة حدوث أعطال او حوادث او كوارث بالنسبة للشبكة وعادة ما تكون عملية النسخ دورية اما أسبوعيا او شهريا ويكون ذلك بطرق آلية من النظام بنفسه. وتعد هذه الطريقة من أهم وأسهل الطرق التي يمكن من خلالها الحفاظ على سلامة المعلومات الخاصة بالشبكات والأنظمة المعلوماتية المتصلة بشبكة الانترنت.