مقاربات حماية أنظمة معلومات المؤسسة من الاعتداءات الالكترونية

أ.د. حديد نوفيل أ. مسوس كمال
جامعة الجزائر3

الملخص :

تتميز بيئة المؤسسة اليوم بالتعقد والديناميكية في مختلف المجالات، أبرزها تلك المتعلقة بتكنولوجيا المعلومات والاتصال وخصوصا تكنولوجيا الانترنت ؛ التي حولت الاقتصاد من اقتصاد قائم على لرأس المال المادي إلى اقتصاد قائم على رأس المال المعرفي، وبفضل هذه التكنولوجيات أصبح للمؤسسة أنظمة معلومات حديثة ومتطورة، لها أهمية كبيرة في خلق القيمة.

لكن ما صاحب استعمال هذه الأنظمة هو تعرضها للعديد من الاعتداءات الالكترونية التي تهدد أمنها وسلامتها كالبرامج الخبيثة، برامج الجوسسة وأسلوب منع الخدمة وغيرها من الاعتداءات، مما جعل المؤسسة تعمل على توفير مختلف الوسائل من أجل حماية أنظمة معلوماتها لضمان سريتها، سلامتها وموثوقيتها كالتشفير الالكتروني، الجدران النارية، التوقيع الالكتروني وغيرها من الوسائل. لكن بالرغم من اعتماد المؤسسة على مختلف الوسائل لتوفير الحماية، إلا أنها لا تزال عرضة لكثير من الاعتداءات الالكترونية، هذا الأمر يتطلب منها تبني مقاربة جديدة تسمح لها بأمن أنظمة معلوماتها بدرجات عالية، ويتجلى تبني المؤسسة لهذه المقاربة من خلال اعتمادها على أحد أو عدد من المعايير والطرق الدولية كمعايير ISO27002،COBIT،ITIL، وغيرها من المرجعيات، هذه الأخيرة سمحت للمؤسسة بالتقليل وبنسب عالية من خطر الاعتداءات الإلكترونية على أنظمة معلوماتها، وبالتالي ساهمت هذه المرجعيات في تحقيق الأهداف الحمائية للمؤسسة"

الكلمات المفتاحية : أنظمة المعلومات الحديثة، الاعتداءات الالكترونية، أمن المعلومات، المرجعيات.

Abstract :

Nowadays, the firm's environment is characterized by complexity and dynamism in different fields, mainly in ICT one. In fact, the most revolution in this field is the internet which transformed the economy from a physical capital-based one to a knowledge–based one and thanks to these technologies; the firm is today endowed with modern and sophisticated information systems which contribute to value creation.

However those systems are exposed to cyber attacks that threat its security and safety such as malwares, spywares, denial of service, etc. To deal with this situation, firms are trying to provide various means like cryptography, firewalls and electronic signature in order to protect their information systems and insure the confidentiality, integrity and availability. In spite of the adoption of those means aiming at information system security, the latter is still vulnerable to cyber attacks. Hence the necessity to adopt a new approach that allows a high information systems security and which is based on international referential as, ISO 27002, COBIT, ITIL, etc. designed to reduce significantly the threat of cyber attacks, and then to enable the firm to achieve its protection objectives.

Key words : modern information systems, cyber attacks, information security, referential.

مقدمة :

تعد أنظمة المعلومات في بيئة الأعمال المعاصرة، من العوامل الهامة والحساسة لنجاح المؤسسات، وهذا نظرا لما تمثله هذه الأنظمة من قيمة إستراتيجية وعنصر هام في سلسلة القيمة لأية مؤسسة، فالحداثة التي تتميز بها اليوم هذه الأنظمة يرجع فيها الفضل للتكنولوجيات الحديثة للمعلومات والاتصال وخاصة تكنولوجيا الانترنت.

إذ أن المؤسسة التي تفشل في الاستفادة من القيمة الكامنة لهذه الأنظمة، تفقد حصة سوقية كبيرة لصالح المنافسين، فضلا عن احتمال خروجها من المنافسة، مما يضع مسألة استمرارية وبقاء المؤسسة رهينة استخدام هذه الأنظمة الحديثة.

إلا أن استخدام الأنظمة الحديثة داخل المؤسسة يجعلها عرضة للاعتداءات الالكترونية المتطورة باستمرار، الأمر الذي يدفع المؤسسات في كل مرة للعمل على توفير مختلف الطرق والأدوات التي من شأنها ضمان السرية، السلامة والتوافر للمعلومات المتواجدة داخل هذه الأنظمة من تلك الاعتداءات.

وعليه سنحاول من خلال هذه المقالة معالجة الإشكالية الرئيسية التالية :

كيف يمكن للمؤسسة الاستفادة من مختلف الوسائل والمرجعيات المعتمدة في أمن أنظمة المعلومات والتقليل من حجم الاعتداءات الالكترونية ؟

من أجل معالجة هذه الإشكالية الرئيسية سنقوم بتناول المحاور التالية :

1- أنظمة المعلومات في ظل التكنولوجيات الحديثة للمعلومات والاتصال ؛

2- الاعتداءات الالكترونية التي تواجهها المؤسسة ؛

3- أمن أنظمة معلومات المؤسسة وشروطه ؛

4- الوسائل المعتمدة في أمن أنظمة معلومات المؤسسة ؛

5- المرجعيات المعتمدة في أمن أنظمة معلومات المؤسسة.

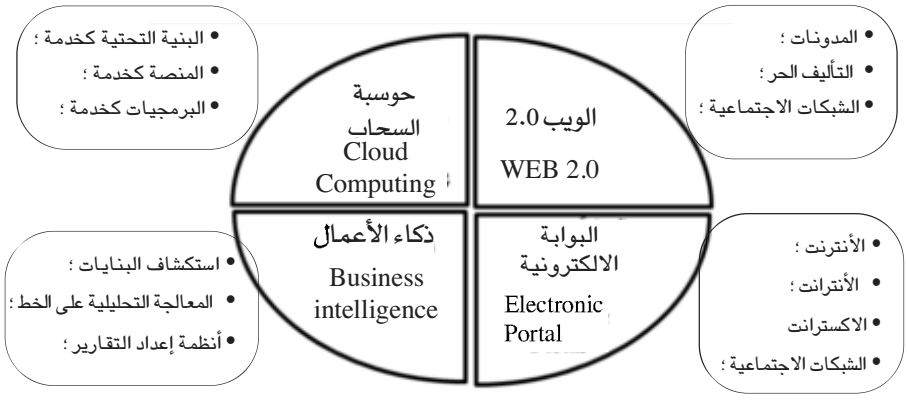
1- أنظمة المعلومات في ظل التكنولوجيات الحديثة للمعلومات والاتصال :

1-1- أنظمة المعلومات الحديثة :

يقصد بأنظمة المعلومات تلك النظم التي تسمح بحجز، تخزين، معالجة، استرجاع، نقل وإيصال المعلومات، للمساعدة على متابعة النشاطات العملية للمؤسسة، وتدعيم اتخاذ القرارات، التنسيق والرقابة وذلك بالاعتماد على تكنولوجيا المعلومات والاتصال وخاصة تكنولوجيا الانترنت. وتعرف أيضا على أنها عبارة عن مجموعة من الطرق، التقنيات والأدوات التي تستعمل من أجل تحيين استغلال تكنولوجيا المعلومات الضرورية للمستخدمين وإستراتيجية المؤسسة[1].

السبب في تسمية أنظمة المعلومات بالحديثة يعود لمواكبة هذه الأنظمة لمختلف التطورات الحاصلة في تكنولوجيا المعلومات والاتصال، التي يمكن توضيح أبرزها في الشكل التالي :

الشكل رقم01: أهم التطورات الحاصلة في تكنولوجيا المعلومات والاتصال



المصدر: من إعداد الباحثين

1-1-1- الويب 2.0 (WEB 2.0) :

تميز الجيل الأول من الانترنت أو ما يطلق عليه بالويب 1.0 بصفحاته ذات القدرة الضعيفة على التفاعل وغيرها من الصفحات الأخرى، هذا الويب تطور إلى جيل ثاني أطلق عليه الويب 2.0، ولم يتوقف الأمر بل استمرت التطورات إلى جيل ثالث (WEB3.0) ورابع (WEB4.0.)

ويعود ظهور مصطلح الويب 2.0 إلى سنة 2004 خلال جلسة عصف ذهني بين Dale Dougherty صاحب منشأة O'Reilly، ومجموعة Craig Cline (Medialive) و John .Battelle (Wired)

إن الويب 2.0 يعني الانتقال من الويب ذات القدرة الضعيفة على التفاعل إلى ويب أكثر ديناميكية أين يعد مستخدم الانترنت منتجا وليس مستهلكا للمعلومات، وتوفير إمكانية تفاعله مع المعنيين بنشر المحتويات.[2] ويقصد به أيضا أسلوب جديد لتقديم خدمات الجيل الثاني من الانترنت، يعمل على تحويل الويب من أداة نشر إلى منصة تعاونية تتيح التعاون، المشاركة بين المستخدمين وتبادل المحتوى عبر الانترنت، وينعكس هذا الأسلوب في مجموعة من التطبيقات أهمها : المدونات (Blog)، التأليف الحرف (WIKI)، النشر المتزامن البسيط (RSS) والشبكات الاجتماعية.[3]

والجدول الموالي يوضح نقاط الاختلاف بين الويب 1.0 والويب 2.0

الجدول رقم01 : الفرق بين والويب 1.0 والويب 2.0

الويب 1.0	الويب 2.0
مواقع شخصية : يقدم من خلالها صاحبها ما يريده هو ويمكن للزوار الاطلاع على محتوياتها.	مدونات : مواقع بسيطة ذات تصميم احترافي تمكن صاحبها من إضافة المقالات (تدوينات) بشكل متقدم، ويمكن للزوار الإطلاع على المقالات والتعليق عليها وحتى تقييمها.
مواقع جماعية : مواقع لا تختلف كثيرا عن المواقع الشخصية إلا أنها تتعلق بمجموعة من الناس هم غالبا أعضاء في مجموعة معينة.	شبكات اجتماعية : تمكن مستخدميها من عمل ملفات شخصية وتبادل التعليقات والتعرف على الأصدقاء وتكوين الجماعات الافتراضية ومن أمثلتها : Face book، MySpace...
مواقع محتويات : مواقع تقدم لزوارها عن طريق صاحبها ملفات مختارة، يستطيع الجميع تنزيلها والاطلاع عليها.	مواقع استضافة ومشاركة ملفات : تقدم لمستخدميها خدمة استضافة الملفات ومشاركتها في الانترنت مع جميع الناس أو مجموعة معينة منهم.
صفحات الأسئلة المتكررة : غالبا ما تكون جامدة لا تتغير وتكون مقدمة عبر إدارة الموقع.	التأليف الحر : مواقع تقدم معلومات بطريقة تشاركيه حيث يستطيع الأعضاء كتابة المقالات والتعديل عليها.
/	خدمة : RSS خدمة لتبادل الأخبار من منتدى أو مدونة أو أي موقع أخر دون الحاجة للوصول إليها

1-1-2- البوابة الالكترونية (Electronic Portal) :

تتضمن البوابة الالكترونية الشبكات التالية :

- **شبكة الانترنت** : هي شبكة عامة تستخدم برتوكول النقل والمراقبة و برتوكول انترنت، يرمز إليهما بـ TCP/IP لتأمين الاتصالات الشبكية، لذا فإنها أوسع شبكة حواسيب في العالم، تزود المستخدمين بالعديد من الخدمات، كالبريد الالكتروني، نقل الملفات، الأخبار، والوصول إلى الآلاف من قواعد البيانات، كذلك تزودهم في الدخول مع حوارات مع أشخاص آخرين في العالم والوصول إلى المكتبات الالكترونية والمجلات وغيرها من التطبيقات والخدمات[4].

- **شبكة الانترانت** : هي شبكة المؤسسة الداخلية أو الخاصة والتي تستخدم تكنولوجيا الانترنت، ويتم تصميمها لمقابلة احتياجات العاملين في المؤسسة من معلومات، ولا يمكن لغير أفراد المؤسسة الولوج أليها[5].

- **شبكة الاكسترانت** : هي عبارة عن شبكة مفتوحة بطريقة أمنة على الشركاء، زبائن وموردي المؤسسة.

- **الشبكة الاجتماعية للمؤسسة** : تعتبر الشبكات الاجتماعية من أهم الحلول الجديدة لأنظمة معلومات المؤسسة، لذا تسعى المؤسسات الحديثة إلى إدراج هذه المنصات التعاونية في إستراتيجية المديرية المعلوماتية، وذلك لتحقيق التكامل مع باقي الأنظمة التقنية الأخرى والمتمثلة في برمجية تخطيط موارد المنشأة ERP، وتبرز مساهمة هذه الشبكات في تحقيق التكامل بين الأنظمة التقنية من خلال[6]:

• **التقاط المعرفة** : من خلال التقاط المعلومات ووحدات المعرفة من المنصات التعاونية والمتمثلة في المدونات، التأليف الحر، المنتديات وغيرها.

• **المشاركة والتعاون** : هذه الشبكات تمكن المؤسسات من التشارك، التحدث والتعاون مع المجتمع الافتراضي، هذا ما أدى إلى ظهور وجه جديد للاتصال يعرف بواحد متعدد. One to Many

1-1-3- ذكاء الأعمال (Business intelligence) :

يهدف ذكاء الأعمال إلى جمع المعلومات عن بيئة المؤسسة بكل مكوناتها، ويعطي المعلومات التي تصف العناصر الموجودة في البيئة اسم الذكاء، مما يسمح باتخاذ أفضل القرارات في أقل وقت ممكن[7]، يعتمد ذكاء الأعمال على ما يسمى بمستودع البيانات الذي هو عبارة عن قاعدة بيانات قرارية تعمل على تخزين مجموعة من البيانات التي تستخدم في إطار عملية اتخاذ القرار والتحليل القراري[8].

يرتكز ذكاء الأعمال على مجموعة من أدوات التحليل والعرض التي من أبرزها :

تنقيب البيانات (Data mining) : هي أداة تعتمد على الذكاء الاصطناعي تساعد على تحليل البيانات المتواجدة على مستوى مستودع البيانات.

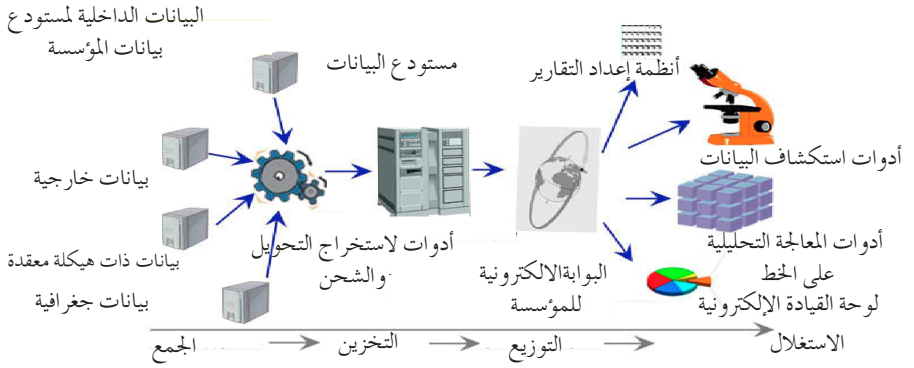
أدوات المعالجة التحليلية على الخط (OLAP): هذه الأداة تسمح بالتحليل على متعدد الأبعاد، وتتم هذه المعالجة بقاعدة بيانات متعددة تكون عادة على شكل مكعب ثلاثي الأبعاد (D3).

– **أنظمة إعداد التقارير (Reporting)** : تسمح هذه الأدوات بإعداد التقارير حسب أشكال معدة مسبقا، ويتم طرح الأسئلة على قاعدة البيانات انطلاقا من مجموعة من الإيعازات SQL يتم إعدادها مسبقا، كما يمكن نشر التقارير دوريا عبر الانترنت أو عند الحاجة.

– **لوحات القيادة (Tableaux de bord)** : تحتوي لوحات القيادة على البيانات الحساسة للمؤسسة وتكون على شكل مؤشرات نصية، بيانية وصوتية. وهي تسمح بإعلام المسؤولين في المنشأة بتطور مستوى النشاطات.

الشكل الموالي يوضح أدوات ذكاء الأعمال السابقة الذكر.

الشكل رقم 02 : ركائز ذكاء الأعمال



Source : http://www.piloter.org/business-intelligence/datawarehouse.htm [2012/05/08]

1-1-4- حوسبة السحاب (cloud computing) :

إن ما يعيق مختلف المؤسسات في الوقت الراهن هو كيفية توفير المال اللازم لشراء مختلف الأجهزة والبرمجيات للقيام بمختلف العمليات المتعلقة بالمعالجة وتحليل البيانات داخل المؤسسة، هذا الأمر أدى إلى ظهور ما يعرف بحوسبة السحاب، هذه الأخيرة تعطي للمؤسسات القدرة على الولوج لمختلف الأجهزة والتطبيقات دون عناء، وبتكاليف مالية جد منخفضة، وهذا مقابل الاشتراك في خدمات إحدى الشركات المختصة في حوسبة السحاب مثل شركة Amazon، وشركة Enomaly وغيرها من الشركات الرائدة في هذا المجال[9].

ولعل أبرز الخدمات التي تقدمها حوسبة السحاب هو الحل SAAS أي البرمجية كخدمة (software as a service)، هذا الحل يسمح للمؤسسة بالحصول على مختلف البرمجيات التي لا تكون على أجهزتها، وذلك عن طريق الدخول للمؤسسات المزودة بهذه الخدمات مقابل اشتراكات مالية[10]، ولعل أبرز الأرقام التي تدل على أهمية هذا الحل هو الدراسة التي قامت بها منظمة ADC التي تتوقع نمو مبيعات تطبيقات SAAS من 13.5 مليار دولار 2009 إلى 40.5 مليار دولار 2014، كما تتوقع نفس المؤسسة انخفاض مبيعات التطبيقات التي تشحن بشكل أقراص مدمجة بنسبة 15% سنة 2012 [11].

2-1 القيمة الاستراتيجية لأنظمة المعلومات وسلسلة القيمة :

تتمثل القيم الإستراتيجية لأنظمة المعلومات في ما يلي[12]:

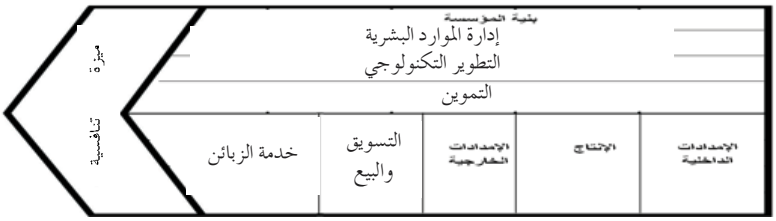
– **القيمة التعهدية (Valeur caution):** تتعلق هذه القيمة بمجرد تبني المؤسسة لنظم معلومات حديثة، فمهما كان استعمالها وتبنيها في المؤسسة، يعطي شرعية اجتماعية للمستثمر وصورة جيدة للمؤسسة.

– **قيمة الاستيعاب (Valeur d'assimilation):** تحتاج قيم الاستيعاب إلى تدخل قوي من طرف النظام الاجتماعي المتبني لهذه النظم الحديثة، فالاستيعاب يتطلب الأخذ بعين الاعتبار للمحيط والميكانيزمات التنظيمية، من خلال تدخل المسيرين بإجراء تخطيط دقيق بين أنظمة المعلومات والتغيرات التقنية، ومن بين أفضل الأمثلة عن قيمة الاستيعاب، نظام تخطيط موارد المؤسسة ERP الذي أثبت فعاليته في مجموعة كبيرة من القطاعات مثل قطاع النقل الجوي وغيره.

– **قيمة التكيف (Valeur d'appropriation):** التي تقوم على التوافق بين النظام المصمم والمستعملين، فهؤلاء وقدراتهم من يحكم الحصول على قيم إستراتيجية من أنظمة المعلومات.

إن القيم السابقة تحقق للمؤسسة اليوم العديد من المزايا كتعزيز الكفاءة التشغيلية، تعزيز جودة المنتج وتعزيز القدرة على الابتكار وغيرها من المزايا، ما جعل المؤسسات الراغبة في تحقيق التميز تدمج أنظمة المعلومات في سلسلة القيمة من خلال دمجها مع الأنشطة الرئيسية والداعمة التي تتكون منها سلسلة القيمة، وفي بعض الأحيان تستخدم أنظمة المعلومات بأشكالها المختلفة كأدوات فعالة لدعم وإسناد الأنشطة الرئيسية التي تضيف قيمة إلى سلع وخدمات المؤسسة بالإضافة إلى أدوارها في تخطيط وتنفيذ الأنشطة المساندة على مستوى الدعم والتنسيق الإداري، وإدارة الموارد البشرية، وتطوير التكنولوجيا ودعم وظيفة الشراء[13].

الشكل رقم03: نموذج Porter لسلسلة القيمة



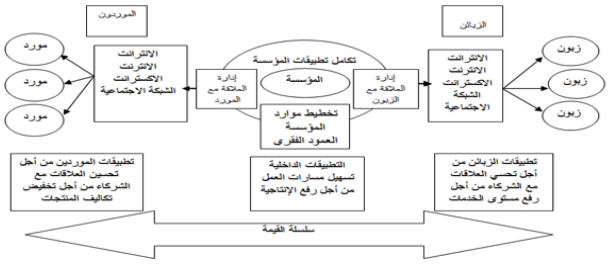
Source : Burg W. D., Evaluer la valeur de l'informatique, la revue n°79, AFAI, 2005, p. 14

إن أنظمة المعلومات تتولى تنفيذ الأنشطة الداعمة في سلسلة القيمة من خلال نظم المعلومات التي تستند على شبكة المؤسسة الداخلية لإدارة تدفقات الأعمال المنسقة بالإضافة إلى دعم أنشطة إدارة الموارد البشرية من خلال نظم معلومات الموارد البشرية وهي من النظم الوظيفية المهمة لنظام المعلومات الإداري. وينطبق نفس الأمر على وظائف تطوير التكنولوجيا من خلال استخدام النظم التي تستند على شبكة المؤسسة الخارجية لأنشطة الهندسة والتصميم بالحاسب وكذلك على وظيفة الشراء حيث تمكن نظم المعلومات المستندة على الويب من تخطيط وتنفيذ أنشطة التجارة الإلكترونية إذا كانت هذه النظم ترتبط بموقع المؤسسة الإلكتروني مع وجود قاعدة بيانات أو مستودع بيانات لتخزين ومعالجة بيانات أنشطة التجارة الإلكترونية[14].

أما على مستوى دعم الأنشطة الرئيسة في سلسلة القيمة، فمن الملاحظ وجود أنماط مهمة من أنظمة المعلومات المستخدمة في مجالات وتطبيقات إمداد المؤسسة بمدخلاتها، أو إدارة وتنفيذ العمليات الإنتاجية باستخدام نظم التصنيع المرنة بالحاسب، أو دعم نظام المخرجات من خلال ربط هذا النظام بنظم المعالجة التحليلية الفورية على الخط، أو بنقاط البيع الإلكتروني والمعالجة الفورية لأوامر الشراء، وهكذا بالنسبة لخدمات الزبائن، ولأنشطة التسويق والمبيعات.

وفيما يلي يمكن توضيح العلاقة التي تربط تطبيقات أنظمة المعلومات وسلسلة القيمة في الشكل التالي :

الشكل رقم04 : علاقة نظم المعلومات بسلسلة القيمة



المصدر : من إعداد الباحثين بالاعتماد على : شهرزاد بن بوزيد، دور تكنولوجيا المعلومات والاتصال في تحسين تنافسية المؤسسات الصغيرة والمتوسطة، رسالة ماجستير، جامعة بومرداس، 2012، ص 120، نقلا عن :

Jean louis Tomas et Guy Bourdellis, ERP et PGI sélection, Déploiement et utilisation opérationnelle, 4éd, Dunod, Paris, 2005, p. 40

نلاحظ من الشكل أن أنظمة المعلومات الحديثة تغطي سلسلة القيمة بصورة كلية، ابتداء من المورد عن طريق برمجية إدارة العلاقة مع الموردين SRM (هذا البرمجية تسمح للمؤسسة بتحسين العلاقات مع مختلف الموردين بما يساهم في خفض تكاليف الإنتاج)، مرورا بالإنتاج من خلال التطبيقات الداخلية للمؤسسة مثل برمجية إدارة دورة حياة المنتج PLM (هذه البرمجية تسمح للمؤسسة بتسهيل كل مسارات العمل مما يساهم في رفع الإنتاجية)، وصولا إلى الزبون من خلال برمجية إدارة العلاقة مع الزبون CRM (هذه البرمجية تسمح للمؤسسة بخلق وتحسين القيمة من خلال كسب ولاء الزبائن والمحافظة عليهم)، أو ككل عن طريق برمجية تخطيط موارد المؤسسة ERP (البرمجية هي عبارة عن نظام متكامل يدمج مختلف التطبيقات في تطبيق واحد وذلك بما يسمح بتكامل البيانات وعدم تكرارها وكذلك تقليص المعالجة مما يساهم في خلق القيمة للمؤسسة).

2- الاعتداءات الالكترونية التي تواجهها المؤسسة :

الاعتداءات الإلكترونية Cyber-attaques هي كل الاعتداءات التي تهدف إلى إلحاق الضرر بأنظمة المعلومات فتؤثر بذلك على سلامة المعلومات، ومصدر توافر المعلومات وسريتها في هذه الأنظمة، هذه الاعتداءات تختلف درجة خطورتها باختلاف الدافع من الاعتداء، فمنها ما يكون بدافع سياسي، اقتصادي أو بدافع تجاري أو فردي ومنها من يقوم بالاعتداء من أجل الفضول والافتخار وغيرها من الاعتداءات، وفيما يلي أهم هذه الاعتداءات :

2-1- الاعتداءات باستعمال البرامج الخبيثة :

هناك العديد من البرامج الخبيثة، التي تستعمل للاعتداء الالكتروني على المؤسسات، ومن مجملها[15]:

- **الفيروسات** : وهي عبارة عن برنامج صغير ينسخ نفسه على أجهزة الحاسب، وله قدرة تخريبية كبيرة تتراوح من إلغاء البيانات أو إلغاء جدول توزيع الملفات إلى عمل خدوش في القرص الصلب نفسه ؛

- **حصان طروادة** : هو برنامج فساد مخفي في برنامج آخر صحيح ويقوم بعمليات فساد تتمثل في إعطاء دخول للحاسوب الذي تشتغل عليه بفتح باب خلفي ؛

- **الهوكس** : وهو ترويج لبعض المعلومات الخاطئة عن طريق البريد الإلكتروني من طرف بعض الجهات، حيث تحرض الرسالة المستقبلة الشخص المستقبل بتحويلها وإرسالها بدوره إلى أشخاص من محيطه. والهدف من هذه العملية هو انسداد الشبكات بسبب التسرب الكبير للمعلومات في نفس الوقت.

- **الدودة** : هي نوع من أنواع الفيروسات الذي تنتشر عن طريق الشبكة، والتي بدون الفيروسات لا يمكنها التكاثر في الشبكة، هذا البرنامج الخبيث يمكن أن يكون على شكل BOT، يتم التحكم فيه عن بعد[16].

2-2- الاعتداءات باستعمال برامج الجوسسة :

برامج الجوسسة تستغل في الاستخدام غير المشروع للمعلومات، من خلال تثبيتها بداخل النظام، حيث تتواصل مع وكيل خارجي عن طريق ما يعرف بالباب الخلفي[17].

بالإضافة إلى ما سبق، هناك مجموعة من الاعتداءات تتم باستعمال أساليب معينة يمكن حصرها في[18]:

2-3- الاعتداءات باستعمال أسلوب اعتراض البيانات :

المقصود بهذا الأسلوب اعتراض وتحليل البيانات المتنقلة بداخل الشبكة بغرض الاستفادة منها بطريقة غير شرعية، يعتمد هذا الأسلوب ببرامج خاصة تدعى .Sniffers

2-4- الاعتداءات باستعمال أسلوب منع تقديم الخدمة:

المقصود هنا بالإضرار المادي بالخادم لمنع تقديم الخدمة، ويعتمد هذا الأسلوب على برامج خاصة تمكنه من تحقيق الأهداف التي يريد تحقيقها تسمى بـ .Flooders

2-5- الاعتداءات باستعمال أسلوب انتحال عنوان : IP

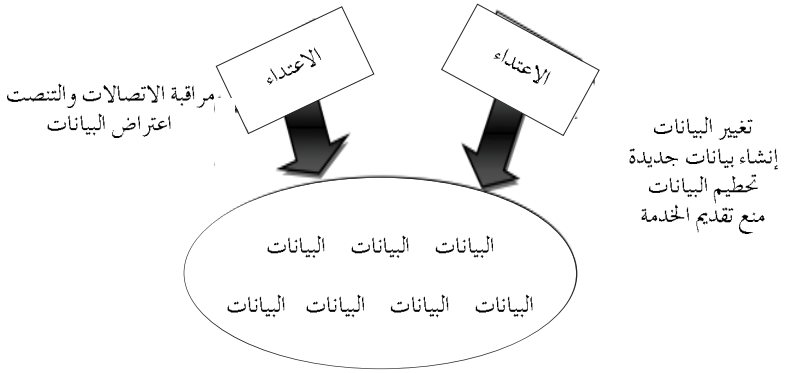
المقصود بهذا الأسلوب تخفي المعتدي، كونه ينتحل صفة مستخدم أخر عن طريق تزوير عنوان IP الخاص به، وهذا ما يسمح له بإخفاء كل أثر يؤدي إلى التعرف عليه في حالة اكتشاف الاعتداء.

2-6- الاعتداءات باستعمال أسلوب انتحال :DNS

المقصود بهذا الأسلوب توجيه مستخدمي الانترنت أوتوماتيكيا إلى المواقع المحتوية على برامج الجوسسة أو المواقع التي تحاكي في تصميمها المواقع التجارية والبنكية، والتي تنجز من قبل المعتدين بغرض الإيقاع بهم.

يمكن تلخيص الأشكال المختلفة للاعتداءات الالكترونية التي يمكن أن تتعرض لها أنظمة معلومات المؤسسة في الشكل التالي :

الشكل رقم05 : الاعتداءات الالكترونية الأساسية التي يمكن أن تتعرض لها المؤسسة



المصدر : من إعداد الباحثين

وللعلم فإن الدراسات المختصة في أمن المعلومات تشير إلى أن حالات الاعتداءات الالكترونية تزداد بشكل خطير على المستوى العالمي، فعلى سبيل المثال، حسب دراسة حديثة

للشركة الأمريكية المختصة في الأمن الالكتروني SYMANTEC فإن عدد الاعتداءات الالكترونية ارتفع بنسبة 71 ٪ سنة 2009 مقارنة بـ 2008 [19].

وتجدر الإشارة إلى أن عدد الأشخاص والمؤسسات الذين تعرضوا للاعتداءات الالكترونية بلغ أرقاماً هائلة ومبالغ مالية جد مرتفعة تمثل ميزانيات بعض الدول، فحسب بعض المختصين في أمن المعلومات وصل عدد الاعتداءات الالكترونية سنة 2013 حوالي 654 870 700 1 اعتداء، في حين وصل حجم الخسائر المالية سنة 2011 فقط حوالي 338 مليار دولار، أما موقع Kaspersky.Lab يشير إلى أن معظم الاعتداءات الالكترونية يكون مصدرها الولايات المتحدة الأمريكية بـ 25.54 ٪، وروسيا بـ 19.44 ٪، وبدرجة أقل هولندا وألمانيا على التوالي بـ 12.80 ٪ و12.51 ٪.

3- أمن أنظمة المعلومات وشروطه:

يعتبر أمن أنظمة المعلومات من الركائز الأساسية التي تأخذها المؤسسات بعين الاعتبار وتضخ له ميزانيات ضخمة، وذلك من أجل التقليل من مختلف المخاطر والاعتداءات الالكترونية التي تواجهها المؤسسات، وبالتالي السماح لها بالتقليل من مختلف الخسائر التي قد تصيبها.

3-1- تعريف أمن أنظمة المعلومات :

لقد وردت العديد من التعاريف التي تخص أمن أنظمة المعلومات نذكر منها على سبيل المثال :

التعريف الأول : أمن المعلومات حسب وكالة الأمن القومي الأمريكي هو حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى المعلومات أو أي تعديل غير مرخص لهذه المعلومات أثناء حفظها ومعالجتها ونقلها، وضد منع تقديم الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف ومواجهة المخاطر والاعتداءات[20].

التعريف الثاني : أمن المعلومات هو عبارة عن الطرق والوسائل المعتمدة للسيطرة على كافة أنواع ومصادر المعلومات وحمايتها من السرقة والتشويه والابتزاز والتلف والضياع والتزوير، والاستخدام غير المرخص وغير القانوني[21].

على أساس التعاريف السابقة يمكن القول أن أمن المعلومات هو حماية البيانات لمنع وصول الأشخاص غير المخول لهم الحصول عليها، وهذه المعلومات أو البيانات تكون سرية وخاصة بالمؤسسة.

3-2- شروط أمن أنظمة المعلومات :

تعتبر ثلاثية CIA من الشروط المهمة جدا في المجالات المتعلقة بأمن المعلومات. ويقصد بـ C.I.A : أولا سرية البيانات (Confidentiality)، ثانيا سلامة البيانات (Integrity) وثالثا توافر البيانات أو الخدمة (Availability). هذه الشروط أو المعايير يمكن توضيحها في الشكل التالي:

- **سرية البيانات** : من خلال العمل على أن لا يطلع عليها من قبل المستخدمين غير المخولين لذلك و غير المرخصين، أو بمعنى أخر حمايتها من الاعتراض والنشر ؛

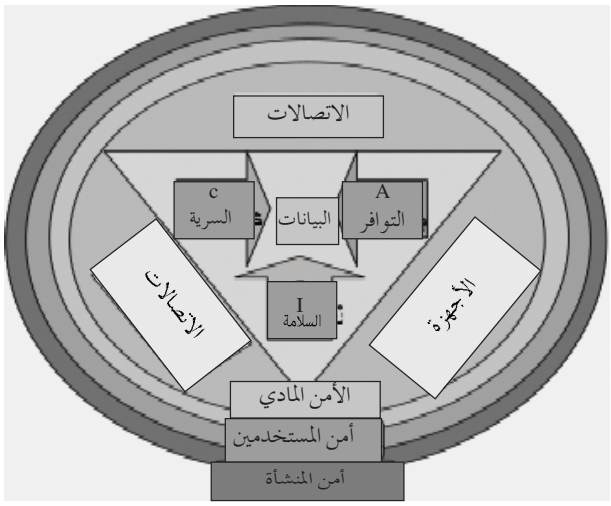
- **سلامة البيانات** : من خلال العمل على أن يبقى المحتوى على حاله دون أي تعديل أو حذف غير مشروعين أو بمعنى أخر ضمان صحتها وكمالها ؛

- **توافر البيانات أو الخدمة** : من خلال العمل على إتاحة كل منهما للمستخدمين المرخصين عند الطلب. بالإضافة للمعايير السابقة، تم إضافة عنصرين جديدين هما[22]:

- **موثوقية البيانات**: وتعني التحقق من هوية المستخدم، أي أن الشخص أو الجهة المتعامل معها هي ذاتها دون لبس أو غموض ؛

– **عدم الإنكار**: ويعني القدرة على ضمان عدم إنكار الطرف المتعامل معه لوقوع المعاملة والنتائج المترتبة عنها، فهي تتعلق بمسؤولية الشخص اتجاه الفعل الذي قد يكون إرسال رسالة أو أي فعل آخر.

الشكل رقم06 : شروط أمن أنظمة المعلومات



http://www.answers.com/topic/information-security

المصدر: من إعداد الباحثين بالاعتماد على :

4- الوسائل المعتمدة في أمن أنظمة معلومات المؤسسة

يستخدم في مجال أمن المعلومات عدة أدوات ووسائل للحماية من المخاطر والاعتداءات الالكترونية، لذا سنذكر أهم هذه الوسائل على النحو التالي :

4-1 التشفير :

التشفير عبارة عن عملية رياضية –معادلات خوارزمية– يتم من خلالها تحويل النص المراد إرساله إلى رموز وإشارات لا يمكن فهمها إلا بعد القيام بفك الشفرة وتحويل الرموز والإشارات إلى نص مقروء من خلال استخدام مفاتيح التشفير العامة والخاصة، فهذه العملية لا تتم إلا إذا كان الطرف الآخر (مستقبل الرسالة) يملك مفتاح التشفير الذي يحول الإشارات والرموز إلى النص الأصلي[23].

ينقسم التشفير إلى نوعين هما :

• **التشفير المتماثل** : ويستخدم فيه المفتاح نفسه للتشفير وفك الشفرة، وبذلك فإن المفتاح يكون معروفًا من قبل كل من مرسل الرسالة ومستقبلها، ولا يتم إرسال المفتاح مع الرسالة ولكنه يرسل بوسيلة أخرى.

• **التشفير غير المتماثل** : يستخدم فيه مفتاحان لكل مستخدم؛ أحدهما مفتاح عام معروف من قبل الآخرين حيث يسجله الشخص عادة مع توقيعه على البريد الإلكتروني وفي حالة الرغبة في إرسال رسالة مشفرة إلى ذلك الشخص يتم استخدام ذلك المفتاح العام لكتابة الشفرة، أما لفكها فيستخدم مفتاح خاص لا يعرفه سوى المستقبل نفسه، ويستخدمه لفك الشفرة المكتوبة باستخدام مفتاحه العام. وعلى الرغم من ارتباط كل من المفتاح العام والخاص ببعضهما إلا أن أي منهما لا يدل على الآخر مطلقًا، فلا يمكن الاستدلال على المفتاح الخاص من خلال العام أو العكس.

4-2 التوقيع الالكتروني : يقصد بالتوقيع الإلكتروني استخدام طريقة أو وسيلة معينة للتحقق من أن صاحب المعاملة هو نفس الشخص الذي قام بإرسالها أو تنفيذها، ويطلق على هذا التوقيع أيضا البصمة الإلكترونية.[24].

4-3 **الشهادة الالكترونية** : هي وثيقة تمنحها الهيئات المختصة في أمن المعلومات تستخدم هذه الشهادة لتحقيق سرية المعاملات من خلال إجراء عمليات التشفير المطلوبة، و كذا التأكد من شخصية كل من المشتري والبائع، وضمان عدم كشف البيانات لكل منهما[25].

4-4 أسلوب الشبكة الخاصة الافتراضية : يعتمد هذا الأسلوب على بروتوكول IPsec، حيث يسمح بإنشاء ممر آمن بين المرسل والمستقبل يتم من خلاله تشفير كل البيانات والرسائل قبل تبادلها[26].

4-5 أسلوب الأمن من خلال نظام : SSL يعتمد هذا الأسلوب على بروتوكول SSL، وهو من إنتاج شركة Netscape الأمريكية سنة 1994، ويسمح بتشفير كل البيانات المتعلقة بالمعاملات التجارية بين الشركة وزبائنها[27].

4-6 الجدران النارية :

يقصد بالجدران النارية النظم التي تحمي جهاز كمبيوتر أو شبكة من أجهزة الكمبيوتر من اختراقات الشبكة من طرف جهة ثالثة ، ويعني ذلك أنه ذلك النظام الذي يسمح بتصفية حزم البيانات المتبادلة مع الشبكة، وهو عبارة عن جسر تصفية يضم على الأقل واجهة لشبكة الاتصال الواجب حمايتها (الشبكة الداخلية) وواجهة لشبكة الاتصال الخارجية[28]، وتنقسم هذه الجدران إلى نوعان هما[29]:

• **الجدران البرمجية** : يمكن استعمال هذا النوع على الحاسبات المستقلة أو الحاسبات المرتبطة بالشبكة أو على الخوادم، ومن أبرز هذه الجدران البرمجية نذكر: Norton internet Security ، Kaspersky internet Security .

• **الجدران المادية** : تسمى كذلك بالعلب السوداء، وهي تستخدم كذلك على الخوادم، وهي أكثر أمنا من الجدران النارية، لكونها غير معنية بنقاط ضعف نظام تشغيل الحاسب، ومن أمثلتها. SOHO WatchGuard .

4-7- البرمجيات المضادة للاعتداءات الإلكترونية : تعد البرمجيات المضادة للاعتداءات الإلكترونية من وسائل أمن المعلومات الأكثر انتشارا ومعرفة من قبل مستخدمي الحواسيب والشبكات، وهي تعمل على البحث عن البرامج الخبيثة التي يمكن أن تتواجد بذاكرة الحاسب أو بأحد وسائط التخزين وتقوم بتحطيمها، كما تعمل على منع تحميل هذه البرامج على الحاسب من خلال أحد أجهزته المحيطية للإدخال أو عبر الشبكة المرتبط بها، كما تعمل كذلك على إيقاف ومنع أغلب الاعتداءات الأخرى كالاعتداءات باستخدام برمجيات الجوسسة، والاعتداءات باستخدام أسلوب اعتراض البيانات وغيرها من الاعتداءات، ومن بين أهم البرمجيات المضادة للاعتداءات الالكترونية نذكر على سبيل المثال[30]:

برمجية Spybot-Search & Destory تسمح بالقضاء على مختلف برامج الجوسسة.

برمجية X-NetStat Professional التي تسمح بالكشف عن حدوث الاعتداء.

5- المرجعيات المعتمدة في أمن أنظمة معلومات المؤسسة:

في وقت قريب كانت الحماية تقتصر على حماية أنظمة المعلومات المتضررة من تخزين للمعلومات ومعالجتها بدلا من حماية المعلومات نفسها، هذا السبب أدى إلى ظهور مجموعة من المرجعيات التي تتعلق بأمن أنظمة المعلومات، كل هذه المرجعيات ترتكز على مجموعة من المقومات التي تندرج ضمن ما يعرف بالحوكمة، كما أن هذه المرجعيات تقترح العديد من التطبيقات الجيدة، تخص جزاء مهما من الحوكمة يدعى حوكمة أمن المعلومات.

إن وجود حوكمة أمن المعلومات داخل المؤسسة أصبح أكثر من ضروري، وهذا راجع لأن أمن المعلومات لم يعد مسألة تخص التقنيين داخل المؤسسة فقط، بل رهان يخص المديرية العامة والمهنية، وبالتالي أصبح من الضروري على المؤسسات الاعتماد على هذه المرجعيات للحد من الاعتداءات الالكترونية، ومن أبرز المرجعيات في أمن أنظمة المعلومات نذكر كل من: ISO، COBIT، ITIL، MEHARI .

5-1 معايير ISO في أمن المعلومات:

تتمثل أهم المعايير ISO المتعلقة بأمن المعلومات فيما يلي:

5-1-1- معيار ISO 27001:

يقدم هذا المعيار العديد من الفوائد للمؤسسات في ما يتعلق بأمن معلومات المؤسسة مثل : تحديد المتطلبات والأهداف الأمنية، التأكد من أن عملية إدارة المخاطر يتم تحديدها بشكل فعال وغير مكلف، تعريف وتوضيح عمليات إدارة أمن المعلومات، تحديد حالة أنشطة إدارة أمن المعلومات بالمؤسسة. كما يمكن أيضا أن يتم استخدام المعيار بواسطة المراجعين الداخليين للمؤسسة أو الخارجيين لتحديد درجة المطابقة والتوافق مع السياسات والتوجيهات والمواصفات المتخذة من قبل المؤسسة[31].

هذا المعيار يقدم نموذج دوري يعرف بـ (PDCA)، وهو اختصار (Plan-DO-Check-Act) يهدف إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل ورصد

واستعراض وصيانة وتحسين وتوثيق نظام إدارة أمن المعلومات داخل المؤسسة وعادة ما ينطبق على جميع أنواع المؤسسات. وكما ذكرنا فإن هذا النموذج يتم في أربع مراحل متتابعة هي[32] :

- الخطة : تأسيس نظام لإدارة أمن المعلومات.
- التنفيذ : البدء في تنفيذ الخطط وتشغيلها.
- التحقق : مراجعة النظام بعد تنفيذه.
- العمل : صيانة وتحسين النظام.

5-1-1- معيار ISO 27002:

هذا المعيار يتضمن السياسات والتوجيهات التالية[33] :

- السياسة الأمنية.
- تنظيم أمن المعلومات يتضمن : تنظيم الأفراد، معرفة أولوية المعلومات و وضع التصنيفات، تقييم المعلومات الجديدة، كيفية الوصول إلى المعلومات من طرف ثالث الاستعانة بالمصادر الخارجية للمعلومات.
- إدارة الأصول.
- أمن الموارد البشرية.
- الأمن البيئي والمادي يتضمن : تنظيم المباني، الحماية من الأخطار المادية مثل الحرائق.
-إدارة الاتصالات والعمليات يتضمن : مراعاة الإجراءات الأمنية للمؤسسة، تنفيذ أنظمة الأمن.
- التحكم في الوصول : تعريف مستويات المستخدمين وحقوق وصولهم، وحقوق إدارة الوقت.
- اقتناء نظم المعلومات وتطويرها وصيانتها.
- إدارة الحوادث الأمنية للمعلومات.
- إدارة استمرارية الأعمال.
- إدارة الامتثال أو التوافق : تتضمن اللوائح التنظيمية، الأحكام القانونية والقواعد الداخلية.

5-1-1- معيار ISO 14508:

يساعد هذا المعيار على التقييم، والتحقق، والتصديق على الضمانات الأمنية للمنتجات التكنولوجية. وكذلك يسمح بتقييم الأجهزة والبرمجيات لمكافحة تغير المناخ في المختبرات المعتمدة للتصديق. كما أن هيكلة هذا المعيار تتم وفق ثلاث منشورات[34]:

- المقدمة والنموذج العام.
- المتطلبات الوظيفية للأمن.
- متطلبات ضمان الأمن.

5-2 مرجعية COBIT:

COBIT هو اختصار لـ Control Objectives for Information and related Technology وتعني أهداف الرقابة الخاصة بالمعلومات وبتكنولوجيا المعلومات، أول نسخة من هذه المرجعية تم تطويرها من قبل جمعية المراقبة ونظم المعلومات ISACA سنة 1994، هذه

المرجعية متطورة باستمرار. أصبحت المرجعية ابتداء من 2003 متوفرة على الويب[35]، وهي حاليا في النسخة الخامسة، هذه المرجعية تقترح العديد من التطبيقات الجيدة على المؤسسة من أبرزها التطبيقات المتعلقة بأمن المعلومات، بالإضافة إلى ذلك تعتبر هذه المرجعية مكملة للمعايير السابقة وذلك من ناحية قياس أمن المعلومات.

تتناول مرجعية COBIT من جانب حوكمة أمن المعلومات العناصر التالية[36]:

- الأخذ بعين الاعتبار لأمن المعلومات داخل الاصطفاف الإستراتيجي ؛
- اتخاذ مختلف التدابير المناسبة للحد من المخاطر والاعتداءات الالكترونية إلى حد مقبول ؛
- المعرفة أو ما يسمى حاليا باليقظة الأمنية، وحماية الأصول ؛
- إدارة الموارد بطريقة تضمن أمن الأنظمة المعلوماتية ؛
- القياس من أجل ضمان أن الأهداف الأمنية تم تحقيقها ؛
- خلق القيمة من خلال تحسين الاستثمارات في مجال أمن المعلومات ؛
- دمج أمن المعلومات داخل سيرورة المؤسسة.

وعلى العموم إطار COBIT يتناول أمن أنظمة المعلومات في أكثر من 20 سيرورة من 34، ولكن السيرورات التالية هي التي تظهر بعدا كبيراً من الناحية الأمنية، وتتمثل هذه السيرورات في[37]:

(**التخطيط والتنظيم** : **السيرورة 05**) : تحقيق الأهداف والاتجاهات الإدارية المتعلقة بالأمن : من بين الأهداف المرتبطة بهذه السيرورة هو ضمان أن المعلومات الهامة سرية ولا يمكن الوصول إليها، بالإضافة إلى التأكد من أن الخدمات والبنية التحتية التكنولوجية قادرة على الصمود في وجه الاعتداءات الإلكترونية.

(**التخطيط والتنظيم** : **السيرورة 08**) : تقييم وتسيير المخاطر: هذه السيرورة تتضمن هدفين أساسيين هما: حماية أصول تكنولوجيا المعلومات والاتصال، وكذلك تحسين البنية التحتية والموارد وقدرات تكنولوجيا معلومات المؤسسة.

(**التوزيع والدعم** : **السيرورة 04**) : ضمان استمرارية الخدمة: هذه السيرورة تتضمن ثلاث أهداف أولها التأكد من أن الخدمات والبنية التحتية التكنولوجية قادرة على الصمود في وجه الاعتداءات الإلكترونية، ثانيا ضمان أن أي حادث مفاجئ لا يؤثر بدرجة كبيرة على أعمال المنشأة وثالثا ضمان أن الخدمات المعلوماتية متوفرة في حالة وجود مخاطر.

(**التوزيع والدعم** : **السيرورة 05**) : ضمان أمن الأنظمة : هذه السيرورة تتضمن هدفين أساسيين هما : حماية أصول تكنولوجيا المعلومات والاتصال، وكذلك أمثلة البنية التحية والموارد وقدرات تكنولوجيا معلومات المؤسسة.

بالإضافة إلى السيرورات السابقة نجد أن مرجعية COBIT تتضمن مجموعة من المعايير متعلقة بأمن أنظمة المعلومات، تتوافق مع المعايير الأساسية المتعلقة بأمن أنظمة المعلومات، والمتمثلة في: السرية، السلامة، والتوافر.

3-5 مرجعية ITIL:

مصطلح ITIL هو اختصار The Information Technology Infrastructure Library، وتعني مكتبة البنية التحتية لتكنولوجيا المعلومات، هذه المرجعية تم تطويرها في أواخر الثمانينات من قبل المنظمة الإنجليزية CCTA (وكالة مركز الحواسيب والاتصالات السلكية واللاسلكية)[38].

هذه المرجعية تتناول أمن أنظمة المعلومات من خلال النسخة الثالثة لها (**ITIL™ V3**)، هذه النسخة تتضمن خمسة مراحل يمكن توضيحها في الشكل التالي

الشكل رقم08 : النسخة الثالثة من مرجعية ITIL

المصدر: يورغ أوكسنر، أفضل إطار عملي وقياس فعلي: ITIL ، ترجمة أبوستروف، الإصدار3، سويسرا 2011، ص 14.

إن أمن أنظمة المعلومات في هذه النسخة يأخذ في مرحلتين أساسيتين[39]:

إستراتيجية الخدمة : هذه المرحلة تقوم بـ :

- تعريف الخطر المتعلق بالحاسب وتحدده عندما يكون هناك عدم يقين في نتائج النشاط؛
- ترجمة هذا الخطر عندما يتم تنفيذ مخطط استمرارية الأنشطة ومخطط تشغيل الأنشطة؛
- عرض المخاطر على أنها سيرورة من سيرورات المراقبة والتقييم.

إن الفهم الجيد لهذه المخاطر في هذا المستوى سيسمح للمؤسسة بالحد منها عندما يتم تحديدها.

- **تصميم الخدمة** : تؤخذ في هذه المرحلة المخاطر المتعلقة بأمن أنظمة المعلومات وفق فصلين أساسيين :
- **تسيير التوافر** : هذا الفصل يعطي مؤشرا على سلامة المعايير المتعلقة بأمن أنظمة المعلومات : السرية، السلامة والتوافر.
- **تسيير أمن المعلومات** : وفق هذا الفصل يتم تحقيق الأهداف الأمنية الداخلية والخارجية عندما يتم استفاء مجموعة من الشروط وهي : السرية، السلامة، التوافر، الحوادث، الخصوصية، الشرعية أو الأصالة.

4-5 طريقة : MEHARI

يتمثل الهدف الرئيسي من تصميم منهجية مهاري في مساعدة مسؤولي سلامة الأنظمة المعلوماتية في مهام إدارة أمن/سلامة نظم المعلومات بغية توفير وسيلة لتحليل وإدارة المخاطر المعلوماتية بأسلوب يتفق مع متطلبات ISO وجميع الموارد والأدوات والمتطلبات لتنفيذها، وعلى هذا تقترح MEHARI منهجية متناسقة، باستخدام قواعد معرفية مشخصة وقادرة على مساعدة المسؤولين على إدارة المؤسسة ومسؤولي السلامة المعلوماتية وكل العناصر في مجال إدارة المخاطر المعلوماتية في مختلف الخطوات والإجراءات وفق المراحل الثلاثة التالية[40]:

– **تحليل وتقييم المخاطر** : يتضمن التحليل المنهجي والآني للحالات التي تنطوي على مخاطر، وتحليل المخاطر في المشاريع الجديدة.

– **تشخيص حالة السلامة المعلوماتية** : تتضمن تشخيص السلامة المعلوماتية كعنصر من عناصر تحليل المخاطر، المخططات الأمنية المبنية على أساس التشخيص، الدعم المقدم من قواعد المعرفة لإنشاء إطار مرجعي للسلامة المعلوماتية، المجالات التي تشملها وحدة التشخيص الأمني.

– **تحليل الرهانات** : يتضمن تحليل الرهانات الأمنية كأساس لتحليل المخاطر وكحجر الزاوية في أي تخطيط إستراتيجي، وتصنيف الأصول كعنصر أساسي لسياسة السلامة المعلوماتية، وتحليل الرهانات الأمنية كأساس للتخطيط الأمني ونظرة عامة حول استخدامات منهجية . MEHARI

الخاتمة :

من خلال هذه الورقة البحثية يمكن القول أن المؤسسات في الوقت الحاضر أمام ضرورة حتمية لتبنى مختلف الوسائل، المعايير والمرجعيات من أجل حماية أنظمة معلوماتها بشكل يضمن لها البقاء والاستمرارية في بيئتها، ذلك نظراً لما توفره هذه الوسائل والمرجعيات والمعايير من تطبيقات تساهم في حماية سرية، سلامة وتوافر المعلومات من الاعتداءات الالكترونية.

الهوامش

3 صلاح الصاوي، سمات الويب 0.2، مجلة مكتبة الملك فهد الوطنية، السعودية، ماي 2012، ص 218.

1 Autssier D. et Delaye V., mesurer la performance de SI, Editions d'organisation, Paris, 2008, p. 49.

2 http://disciplines.ac-bordeaux.fr/.../Les%20mots%20du%20Web%202%200.pdf [2012/10/24]

4 إيمان السامرائي وآخرون، مصادر المعلومات التقليدية والالكترونية، دار اليازوري، الأردن، عمان، 2009، ص 599.

5 ثابت عبد الرحمان إدريس، نظم المعلومات الإدارية في المنظمات المعاصرة، الدار الجامعية، مصر 2005، ص 497.

6 Dijoux C., Positionnement dans le SI : Entreprise 2.0, livre blanc collectif et collaboratif publication coordonnée par anthony poncier, 2010, p.p. 14-19

7 نوفيل حديد، الإدارة الحديثة للأعمال في مواجهة تغيرات العصر ومستجداته، مجلة الاقتصاد والتكنولوجيا، بن عكنون، العدد 04، 2011، ص 28.

8 http://www.piloter.org/business-intelligence/datawarehouse.htm [2012/05/08]

9 بودريسة نوال، حوسبة السحاب، مجلة الاقتصاد والتكنولوجيا، الجزائر، بن عكنون، العدد 10، نوفمبر 2011، ص 13–14.

10 www.afai.fr/public/doc/516.pdf [2014/02/20]

11 بودريسة نوال، نفس المرجع، ص 17.

12 شهرزاد بن بوزيد، دور تكنولوجيا المعلومات والاتصال في تحسين تنافسية المؤسسسات الصغيرة والمتوسطة، رسالة ماجستير، جامعة بومرداس، 2012، ص 105.

13 عبد الحميد عبد الفتاح المغربي، نظم المعلومات الإدارية، الدار الجامعية مصر الإسكندرية، 2002، ص 71.

14 كورتيس جراهام، ترجمة علي يوسف على، تحليل وتصميم نظم المعلومات، دار خوارزم، القاهرة، 1998، ص 73.

15 http://www.commentcamarche.net/contents/virus [2012/10/20]

16 Bloch L., Wolfhugel C., Sécurité informatique, Eyrolles, Paris, 2008, p. 60

17 IBID, p. 60

18 نوفيل حديد، مرجع سبق ذكره،2007 ص 80.

19 http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20100420_02 [2012/08/22]

20 GOMEZ URBINA A. et autres, Hacking interdit : Toutes les techniques des hackers enfin décryptées pour ne plus jamais vous laisser piéger !, Micro application, Paris, 2006, p. 724

21 إيمان فاضل السامرائي و هيثم محمد الزغبي، مرجع سبق ذكره، ص 283.

22 Ghernaouti Hélie S., Sécurité informatique et réseaux, Dunod, Paris, 2008, p. 2

23 محمد فواز محمد، الوجيز في عقود التجارة الإلكترونية، دار الثقافة النشر والتوزيع، عمان، 2006، ص 159.

24 نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة النشر والتوزيع، عمان، 2005، ص 84.

25 حسن نوبي محمد، منظومة الحكومة الإلكترونية، المعهد العربي لإنماء المدن،ندوة الحكومة الإلكترونية : الواقع والتحديات،صنعاء،2003، ص 128.

26 نوفيل حديد، مرجع سبق ذكره،2007، ص 187.

27 المرجع نفسه، ص 187.

28 http://www.commentcamarche.net/contents/protect/firewall.php3 [15/07/2012]

29 نوفيل حديد، مرجع سبق ذكره، 2007، ص 186.

30 المرجع نفسه، ص 184.

31 قسم الجودة والتطوير، إيزو 27001، ط2، المركز القومي للمعلومات، السودان، إ1، 2010، ص 3.

32 Moisand D., COBIT pour une meilleure gouvernance des SI, Editions, Paris, 2009, p. 15

33 Moisand D., 2009, op.cit, p. 15

34 IBID, p 17.

35 Hardy G., Gulden E., Le nouveau visage de CobiT, Référentiel CobiT, la revue de Afai, n°82, 2006, p. 27

36 Moisand D., COBIT pour un meilleure GSI, Eyrolles, Paris, 2éd, 2010, p. 214

37 IBID, p 70, 86, 141,161.

38 Gmish, Fiches de synthèse relative aux démarches de gouvernance SI, v1, 2007, p. 6

39 يورغ أوكسنر، أفضل إطار عملي وقياس فعلي: ITIL ، ترجمة أبوستروف، الإصدار3، سويسرا 2011، ص 14.

40 .Jouas J. Ph, Roule J. l., MEHARI 2010, club de la sécurité de l'information, Paris, 2010, p.p. 3-4