المخاطر الالكترونية التي تواجه المؤسسة ووسائل الأمن الواجب اعتمادها

The electronic risks facing the institution and the means of security to be adopted

بوالفول هرون [1]♦

[1] أستاذ محاضر، جامعة الجزائر3، الجزائر، الإيميل: harounee@yahoo.fr

تاريخ الاستلام: 2017-12-18 تاريخ القبول: 2018-12-04 تاريخ النشر: 2018-12-12

ملخص:

تجابه قطاعات الأعمال الحديثة في العالم أجمع هذه الأيام تحديات هامة يأتي في مقدمتها حماية معلوماتها الإلكترونية، والتي تشمل العديد من الأمور منها البيانات التي تتبادلها المؤسسات وتعاملاتها عبر الإنترنت، واستخدامات العاملين والموظفين فيها لبنيتها التحتية المعلوماتية. إلا أنه وللأسف فإن هذا الأمر مازال لا يحظى بالاهتمام المطلوب من المديرين وصناع القرار في الكثير من المؤسسات، بل نستطيع القول إن غالبية المؤسسات والشركات تفتقر إلى أنظمة حماية عالية الكفاءة لحماية أهم ما تمتلكه هذه المؤسسات، ألا وهو معلوماتها. ويعود السبب في هذا التجاهل النسبي لأهمية الحماية الإلكترونية للبيانات في المؤسسات في الواقع إلى افتقار المعرفة الكافية بما تتطلبه عملية توفير الحماية الصحيحة للبيانات، ومن خلال هذه الورقة يتم التطرق إلى المخاطر الالكترونية التي تواجه المؤسسات ووسائل الأمن الواجب إعتمادها

كلمات مفتاحية: امن المعلومات، المخاطر الالكترونية.

تصنيف JEL : D80

Abstract:

Facing modern business sectors in the entire world, these days comes significant challenges in the forefront of protecting their information online, which include many of the things which the data exchanged between institutions and transactions over the Internet, the uses of workers and staff working in the IT infrastructure. But unfortunately this still does not have the attention required of managers and decision-makers in many of the institutions, But we can say that most of the institutions and companies lack the protection of high-efficiency systems for the same institutions, namely information. The reason for this relative neglect of the importance of electronic data protection in the institutions, in fact to the lack of sufficient knowledge as required to provide the correct data protection process, and through this paper addressed to the electronic risks by institutions and means of security must be adopted it

Keywords: information security, e-risk.

JEL Classification: D80

♦المؤلف المرسل: بوالفول هرون، الإيميل: harounee@yahoo.fr

1.مقدمة:

مع التطور التقني الذي نعيشه وتسارعه، أصبح الأمر أكثر إلحاحا من أي وقت مضى لاستخدام الأجهزة التقنية، وتبادل المعلومات عن طريق الانترنت واللجوء إلى حفظ هذه البيانات وتخزينها الكترونيا، وبذلك يكون هذا التطور سببا مهما في تسهيل الحاجة لحفظ هذه المعلومات وإمكانية استردادها، كما أصبح ذات السبب يشكل خطرا حقيقيا في وجه أمن وسلامة تلك المعلومات، ولأجل ذلك فإن موضوع حماية أمن المعلومات اليوم ازداد أهمية ومع تقدم الوقت بالنسبة للإفراد وبنسبة أكبر للشركات كونها تنظيم مهم وركن أساسي في قطاع حيوي كقطاع الأعمال، والهجمات الالكترونية تأتي في الصف الأول كأكبر التهديدات التي تؤثر على سلامة هذه المعلومات على الشبكة، ودخلت بقوة لقائمة المخاطر المستهدفة لقطاع الأعمال، لذا يمكننا أن نطرح الإشكالية التالية: ما هي أهم الهجمات الالكترونية التي تتعرض لها المؤسسة، وأهم الوسائل التقنية المعتمدة في أمن الأعمال الالكترونية؟

وللإجابة عن الإشكالية سنقسم هذا البحث إلى ثلاث محاور:

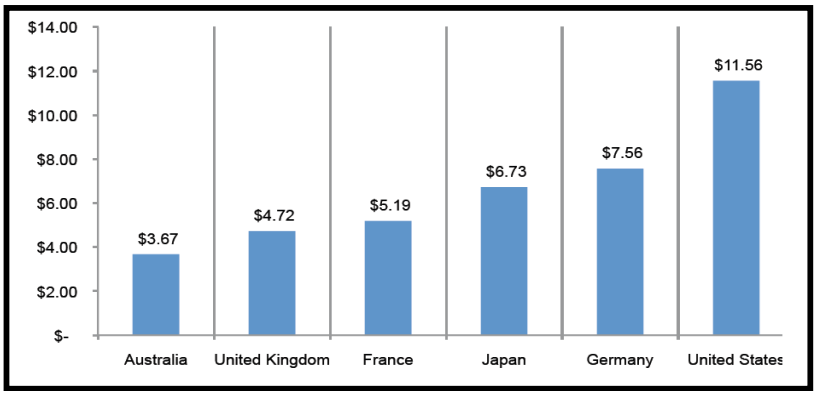
- مفهوم أمن المعلومات ومكوناته.
- الهجمات الالكترونية التي تتعرض لها المؤسسة.
- أهم الوسائل التقنية المعتمدة في أمن الأعمال الالكترونية.

2. مفهوم أمن المعلومات ومكوناته

أجريت الدراسة[1] السنوية لعام 2013 في الولايات المتحدة والمملكة المتحدة وألمانيا وأستراليا واليابان وفرنسا مع عينة مرجعية إجمالية قدرها 234 منظمات، هذا وتم عرض هذه النتائج العالمية في مخطوط منفصل تحت عنوان تكلفة الجرائم الإلكترونية لسنة 2013: تقرير عالمي، ويبين الشكل رقم (10) متوسط التكلفة التقديرية للجرائم الإلكترونية لعينات من ستة دول شاركت فيه 234 شركة منفصلة، هذا وتم تحويل هذه الأرقام إلى الدولار الأمريكي وذلك لغرض المقارنة، وكما هو مبين يوجد تباين كبير في التكاليف الإجمالية لجرائم الإلكترونية مابين الشركات المشاركة في العينات المرجعية، حيث تبين عينة الولايات المتحدة أعلى نسبة متوسط التكلفة بقيمة تبلغ 11560000 دولار، في حين تبين العينة الاسترالية أدنى إجمالي متوسط التكلفة بقيمة تبلغ 3670000 دولار.

الشكل رقم 01: التكلفة الإجمالية للجرائم الإلكترونية في ست دول.

تم حذف التكلفة المعبر عنها بالدولار الأمريكي $ 1000000



المصدر: Ponemon Institute, Research Report,(2013) Cost of Cyber Crime Study:United States, Sponsored by HP Enterprise Security Independently conducted by Ponemon Institute LLC Publication Date: October 2013,p:2.

قد تعود الأسباب المحتملة لهذه الاختلافات لأنواع وتواتر الهجمات التي حدثت، هذا فضلا عن الأهمية التي توليها كل شركة لسرقة أصول المعلومات وذلك مقابل عواقب أخرى عن الحادث، وقد خلصت هذه الدراسة إلى أن الشركات الأمريكية هي أكثر عرضة لتشهد أغلى أنواع الهجمات الإلكترونية والمتمثلة في الشفرة الخبيثة والحرمان من الخدمة والحوادث على شبكة الإنترنت، نفس الشيء بالنسبة لأستراليا التي تعتبر أكثر عرضة لتشهد هجمات الحرمان من الخدمة، وعلى النقيض من هذا تعتبر الشركات الألمانية أقل عرضة لتشهد هجمات الشفرات الخبيثة، أما فيما يتعلق بالشركات اليابانية فتعتبر أقل عرضة لتشهد هجمات سرقة الأجهزة وهجمات الشفرات الخبيثة، نتيجة أخرى مهمة خلصت إليها من شأنها أن تفسر هذه الاختلافات الموجودة ما بين الدول وتتعلق بسرقة أصول المعلومات، حيث تفيد الشركات الأمريكية واليابانية والألمانية أن هذه أهم عاقبة للهجمات الإلكترونية، من جهة أخرى تعتبر المملكة المتحدة وفرنسا واستراليا تعطل الأعمال التجارية أكثر أهمية، ويبين تحليل تكاليف النشاط الداخلي اختلافات جد مهمة على وجه التحديد تبدو تكلفة الكشف والتعافي من الهجوم الإلكتروني الأعلى بالنسبة للشركات الأمريكية والفرنسية واليابانية والألمانية، ومع ذلك فإن تكلفة التعافي من الهجمات الإلكترونية تعتبر أيضا مكلفة بالنسبة للشركات في أستراليا والمملكة المتحدة، ومن الجدير بالذكر أن نشير إلى أن الشركات اليابانية تخصص تكاليف باهظة للتحقيق وإدارة الحوادث أكثر من البلدان الأخرى، وكما يوضح الجدول التالي لأكبر الهجمات الالكترونية على الدول في العالم:

الجدول رقم 01: الدول الأكثر عرضة للهجمات الالكترونية

الدولة	الربع الأول 2010(%)	الربع الثاني 2010(%)
أمريكا	10	11
الصين	9,1	11
روسيا	12	10
تايوان	6,1	6
البرازيل	6	6
ايطاليا	4,4	3
المانيا	3,9	3
رومانيا	3,2	3
اليابان	2,9	3
تركيا	1,5	3

المصدر: Akamai, the state of Internet, (Vol. 3, No.22nd Quarter), 2010, p: 7.

1.2 مفهوم أمن المعلومات: هو عبارة عن برامج خبيثة قد تتكاثر آلياً أو لا تتكاثر، وتتصف بالنّزعة الهجومية وتستقر على نظام معلومات المؤسسة من أجل إصابته وإلحاق الضرر بسّرية أو سلامة أو توفر معلومات هذا النِّظام، أو من أجل تجريم مستعمله والقيام بجريمة ما[2]، وأمن المعلومات على أنه "حماية المعلومات ونظم المعلومات من الولوج الغير المسموح به والاستخدام والكشف أو الخلل والتغيير والتدمير[3]"، هذا يعني أننا نود حماية بياناتنا وأنظمتنا من أولئك الذين يحاولون إساءة استخدامها،

والأمن قد يعني عموما حماية أصولنا، وهذا قد يعني حمايتهم من المهاجمين الدين يغزون شبكاتنا والكوارث الطبيعية والظروف البيئية المعاكسة وانقطاع التيار الكهربائي والسرقة والتخريب أو الكشف عن هذه البيانات من قبل دول أخرى غير مرغوب فيها، وفي نهاية المطاف فنحن سنسعى قدر المستطاع لتأمين أنفسنا من أكثر الأشكال المحتملة للهجمات وذلك حسب بيئتنا، وعندما نتمعن فيما يجب علينا بالضبط أن نؤمن، قد تكون لدينا مجموعة واسعة من الأصول المحتملة، ويمكن لنا أن نأخذ بعين الاعتبار العناصر القيمة لأعمالنا (على سبيل المثال الأجهزة الحاسوبية) وقد تكون لدينا أيضا عناصر ذات طابع مادي مثل البرمجيات وشفرة المصدر أو البيانات، وفي بيئة الحوسبة اليوم من المرجح أن نجد أن أصولنا المنطقية هي على الأقل ذات قيمة هذا إن لم تكن أكثر من أصولنا المادية، إضافة إلى كل هذا يجب علينا كذلك حماية الأشخاص المنخرطين في عملياتنا، فالأشخاص يمثلون بالنسبة لنا أهم قيمة فنحن عموما لا يمكننا إجراء الأعمال التجارية بدونهم، وفي أي بيئة أين نخطط لتطبيق مستويات عالية من الأمن، يجب كذلك أن نأخذ بعين الاعتبار تكلفة استبدال أصولنا في حالة فقداننا لها، ونتأكد من أن تحديد مستويات الحماية تتماشى وقيمة هاته الأصول، فتكلفة الأمن التي نطبقها لا ينبغي أبدا أن تفوق قيمة ما يتم حمايته.

2.2 مكونات أمن المعلومات الالكترونية:

- **سرية المعلومات:** وهذا الجانب يشتمل على الإجراءات والتدابير اللازمة لمنع إطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وهذا هو المقصود بأمن وسرية المعلومات، وطبعاً درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب سريتها: المعلومات الشخصية للأفراد، الميزانية المالية للشركات قبل إعلانها، المعلومات والبيانات العسكرية الخاصة بالجيوش والمواقع العسكرية في البلاد.
- **سلامة المعلومات:** في هذا الجانب لا يكون الهم الأكبر هو الحفاظ على سرية المعلومات وإنما يكون الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان عن معلومات مالية أو غيرها تخص الهيئة وهنا يأتي دور الحفاظ على السلامة بأن تكون هذه المعلومات محمية من التغيير أو التزوير، وإن الإخلال بسلامة البيانات ليس بالضرورة نتيجة عمل تخريبي، فمثلاً الانقطاع في النظام قد ينشئ عنه تغيرات غير مقصودة أو لا تحفظ تغيرات قد تمت فعلا[4].
- **ضمان الوصول إلى المعلومات:** من المنطقي أن نعرف إن كل إجراءات وصناعة المعلومات في الأساس تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات إلى الأشخاص المناسبين في الوقت المناسب، وبالتالي فإن الحفاظ على سرية المعلومات وضمان سلامتها وعدم التغيير فها لا يعني شيئاً إذا لم يستطع الأشخاص المخولون أو المصرح لهم الوصول إليها، وهنا تأتي أهمية الجانب الثالث من جوانب أو مكونات أمن المعلومات وهو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، وفي هذا الجانب يعمل المخربون بوسائل شتى لحرمان ومنع المستفيدين من الوصول إلى المعلومات مثل حذف المعلومات قبل الوصول إليها أو حتى مهاجمة أجهزة تخزين المعلومات وتدميرها أو على الأقل تخريبها.

3. الهجمات الالكترونية التي تتعرض لها المؤسسة

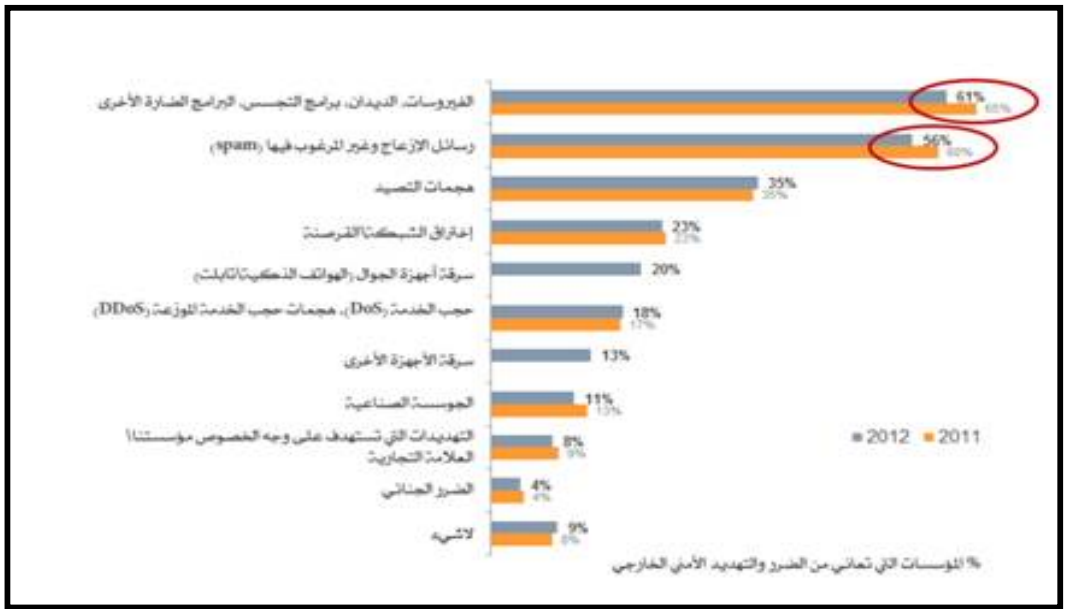
1.3 الإعتداء بإستعمال البرمجيات الخبيثة (Malware): البرمجيات الخبيثة هي برامج مؤذية يمكن أن تلحق الضرر بأنظمة حواسيب المنزل والمكتب والعمل، وغرض المهاجم الالكتروني هو أن يكون قادرا على الدوام على التحكم الكامل في

المعلومات السرية للعميل مثل: بطاقة الائتمان، الاسم، البريد الإلكتروني، أرقام الضمان الاجتماعي من أجل سرقة هويات الناس أو أموالهم وعلى سبيل المثال: ثمة برمجية خبيثة تدعى تسونامي طروادة Tsunami Trojan، ومعظم الضرر الذي يلحقه تسونامي طروادة يكون بالنافذة مثل: ماك يونيكس Mac UNIX ويستخرج منصة تستطيع زيادة قاعدة المستخدم يتابع احتمال استغلال نقاط الضعف[5]، ومن الأمثلة الشائعة على البرمجيات الخبيثة ما يلي:

- **الفيروسات:** تعد أخطر من البرامج التي قد تدمر الأجهزة تدميرا تاما، حيث يعتبر نوعا من برامج الحاسب الالكتروني التي ترسل إشارات داخل كود أو السجلات والمطبوعات، كما تعتبر أحد أنواع الحرب المدمرة للمعلومات[6].
- **الديدان:** مثلها مثل الفيروسات، حيث أنها عبارة عن برامج تقوم بمضاعفة نفسها بشكل مستقل ولكنها لا تقوم بربط نفسها بأي ملفات خارجية أو إصابة أي ملفات جديدة. وبعبارة أخري هي عبارة عن برنامج صغير مكتوب بإحدى لغات الحاسب مصمم على أن يقوم بإعادة كتابة نفسه على الملفات الموجودة على الحاسب أو أي حاسب أخر، ولكنها متميزة بكونها ترسل نفسها منفردة إلى قائمة البريد الالكتروني إلى كل جهاز بالشبكة وهى تنتشر بسرعة هائلة[7].
- **برنامج Macro**: مصمم للعمل على تطبيق معين أو لعدة تطبيقات تشترك بلغة برمجة واحدة مثل word, excel فعندما يتم فتح الوثيقة المصابة فإن الفيروس ينشط ويؤدي مهمته التخريبية، وله القدرة على نسخ نفسه إلى ملفات الوثائق الأخرى، مما يساعد في زيادة إنتشاره مع استمرار استخدام البرنامج[8].
- **أحصنة طروادة:** وهى عبارة عن برامج خبيثة تصيب النظام والفرق بين أحصنة طروادة وبين الفيروسات والديدان هو أن أحصنة طروادة لا تقوم بالتكاثر ذاتيا، وقد تم اشتقاق اسم حصان طروادة من الأساطير اليونانية، وهذه البرامج تكون بريئة المظهر من الخارج ولكن محتواها يكون خبيثا وهي تصيب النظام عند تنفيذها، والغرض الرئيسي من أحصنة طروادة هو تعريض النظام المصاب إلى الخطر، ويوجد العديد من أحصنة طروادة حيث يكون بعضها بمثابة الباب الخلفي للنظام أو يكون الغرض من أحصنة طروادة التجسس على المستخدم أو تنزيل بعض البرامج الخبيثة إلى النظام[9].

وحسب دراسة[10] التي قامت بها Kaspersky بالتعاون مع B2B international بينت أن التهديدات الخارجية الأكثر شيوعا والتي واجهت المختصين في تقنية المعلومات كانت البرامج الخبيثة وبنسبة 61% كما هو مبين في الشكل التالي :

الشكل رقم 02: المؤسسات التي تعانى من الضرر والتهديد الأمني الخارجي



المصدر: Kaspersky, Research Report, Global IT Security Risks: 2012, p:4

2.3 الإعتداء بإستعمال أسلوب انتحال عنوان IP : تقوم معدات الشبكات مع نظام شغال باستخدام عنوان IP لجهاز كمبيوتر من أجل تحديد عنوان ساري المفعول، حيث يمكن تعديل عنوان IP لزبون من قبل مهاجم من أجل التمكن من قراءة وكتابة المعلومات الخاصة به، يمكن أيضا للمهاجم استخدام تطبيق خاص للتلاعب بحزم IP التي تنشأ عن عناوين سارية المفعول داخل انترنت الشركة، فمن الأسهل للمهاجمين بعد الوصول إلى الشبكة كنتيجة لتعديل عنوان IP الساري المفعول إعادة كتابة أو حذف المعلومات[11].

3.3 الإعتداء بإستعمال أسلوب "اعتراض البيانات": يستخدم مهاجم Sniffers تطبيقا أو جهازا لقراءة وإعادة كتابة ومراقبة والاستيلاء على مبادلات معلومات الشبكة خلال إرسال الطرود، وفي حالة ما إذا لم يكن الطرد مشفرا بشكل جيد فسيتمكن المهاجم عن طريق Sniffers من رؤية البيانات الموجودة داخل الطرد، وحتى الطرود المغلفة يتم قراءتها من قبل المهاجم إن لم تكن مشفرة، فحينها لا يمكن للمهاجم الوصول إلى البيانات الرئيسية، ويقوم المهاجم بتحليل الشبكة والحصول على معلومات وذلك للتسبب في نهاية المطاف في تعطيل الشبكة وإفسادها وأيضا قراءة طرد IP المرسل عبر الاتصالات[12].

4.3 الإعتداء بإستعمال أسلوب "منع تقديم الخدمة"(DOS): يتم في هذا النوع من الهجمات إرسال عدد كبير من الشبكة الخارجية (عادة الانترنت) إلى الشبكة الداخلية[13]، وهجوم رفض الخدمة يمنع الاستخدام العادي للحسابات السليمة في الحاسوب، وينجز الوظائف التالية:

- يوزع عشوائيا انتباه الطاقم الإداري بحيث لا يعلمون بالتهديد مباشرة، مما يسمح للمهاجم بتنفيذ الهجمات تباعا أثناء إلهائه إياهم.
- يبعث أيضا تطبيقات أو خدمات شبكية غير سليمة تتسبب في قابلية التطبيقات للأنهيار.
- يغرق شبكة الحاسوب بأكملها بالرزم إلى غاية توقف الحاسوب عن العمل بسبب الحمل الزائد.
- يعطل المرور بسبب انعدام الوصول إلى موارد الشبكة من قبل مستخدمين مرخص لهم.
- وهجوم رفض الخدمة خاص وسط جميع التهديدات الأخرى التي تهاجم المواقع الإلكترونية الكبيرة على الانترنت، ويقرصن رفض الخدمة النظام المصمم لجلب الشبكة لكشف الأداة الإلكترونية بإغراقها برزمة غير لازمة، يمكن حصول رفض الخدمة عندما يُغرق نظام – خادم أو قاعدة بيانات مثلا – بطلبات غير مبررة تجعله غير قادر على الاستجابة للمهام الحقيقية على سبيل المثال، ياهو، أم أس أن، فايسبوك، وإياي كانوا جميعا ضحايا لما يلي:
- أداء بطيء للشبكة،
- تقييد حقوق المستخدم في الدخول لأي موقع،
- زيادة كارثية في استقبال (Spam) في حساب البريد الالكتروني، وهذه الأيام يعتبر البريد العشوائي من التهديدات الخطيرة لمؤسسات الأعمال والبنية التحتية في ظل استخدامه بواسطة البائعين والمسوقين كأحد الطرق المستحدثة للوصول إلى العملاء الحاليين والمرتقبين[14].

5.3 الإعتداء بإستعمال أسلوب تغيير البيانات: يستخدم المهاجم برمجيات متطورة من أجل جمع البيانات واختراق أمن الشبكة، حيث يرسل مهاجم (اتصال MTM) رسالة وهمية من أجل تشكيل شبكة الزبون (الضحية) والتظاهر على أنه مزود خدمة الإنترنت قانوني، هذا ويشير مكتب التحقيقات الفيدرالي الأمريكي أحيانا إلى المتطفلين أو القراصنة على أنهم مجرمين

وذلك لأنهم متورطون في جرائم مختلفة عبر الإنترنت مثل استغلال المعلومات القيمة وسرقة الوثائق والوصول إلى قواعد البيانات بشكل غير قانوني، هذا وتنشأ التهديدات على أي شبكة كلا من الكيانين الخارجي والداخلي على غرار المستخدمين غير المخولين (الهاكرز) وهجمات الفيروسات وجهل الآخرين، وجميع البيانات التي استغلت وتم تغييرها وإعادة كتابتها أو قراءتها عن طريق الهجوم وذلك دون علم المالك الشرعي، على سبيل المثال: الضحية هو الشخص الذي قام المستخدمون غير المرخص لهم باستغلال معلومات جهاز الكمبيوتر الخاص به[15]، وتؤدي إلى ارتكاب العديد من الجرائم الالكترونية، وفقد المعلومات السرية الحرجة إضافة إلى تشويه سمعة وشهرة المؤسسة[16].

6.3 الهجمات عن طريق كلمة المرور: في هذه الوضعية يقوم المهاجم بالاستيلاء على حساب ساري المفعول للمستخدمين الأصليين ويدعي أنه المالك الشرعي للحساب، وذلك لكي يتمكن من تنفيذ نفس حق المستخدم الأصلي، وعليه فإن كلا من المستخدم الشرعي والمهاجم يتمتعان بنفس الحق، وعلى سبيل المثال: إذا كان للمستخدم حقوق إدارية، فإن الهاكرز أيضا يقومون بإنشاء حسابات للولوج في وقت واحد، وبإمكان المتطفل القيام بالمهام التالية[17]:

- كانت برمجية آلة حاسبة كلمة المرور أحدى الطرق المطلوبة لهجوم القوة الغاشمة.
- تغيير عناوين IP وتكوينات شبكة الاتصال بما في ذلك الوصول للتحكم في عنوان MAC وجداول التوجيه.
- تعديل وإعادة كتابة أو حذف معلومات قيمة.

7.3 الإعتداء بإستعمال أسلوب انتحال نظام أسماء النطاقات (DNS): المقصود بهذا الأسلوب توجيه مستخدمي الإنترنت أوتوماتكياً إلى المواقع المحتوية على «برامج الجوسسة» أو المواقع التي تحاكي في تصميمها المواقع التجارية والبنكية الحقيقية والتي تنجز من قبل المعتدين بغرض الإيقاع بهم، ويتم هذا التوجيه من خلال الرسائل الالكترونية غير المرغوب فيها[18].

8.3 الهجوم على طبقة البرامج التطبيقية: يستهدف هجوم على طبقة البرامج التطبيقية خوادم التطبيقات بإستعمال تكنولوجيا خاصة لفك رموز نظام التشغيل أو كلمة السر وهذا يمكّن هجمات قراصنة الشبكات اللاسلكية من الحصول على إمكانية تجنب مراقبات الدخول إلى شبكة معينة. يستفيد المهاجم من هذه الوضعية بالتحكم في التطبيق أو النظام أو الشبكة، ويقوم بتنفيذ المهام التالية:

- تنفيذ برنامج فيروس يستعمل تطبيقا برمجيا لإطلاق الفيروسات عبر الشبكة.
- إدخال برنامج مراقب الشبكة لرصد معلومات الشبكة التي يحتمل أنها تستعمل كأداة فك الرموز لتدمير الشبكة.
- إتلاف التطبيقات والبرامج بشكل غير طبيعي.
- تعطيل مكونات الأمان في الشبكة لتمكينه من التحكم مستقبلا والدخول إلى الشبكة.

9.3 تهديدات كشف المفتاح: المفتاح هو الرمز أو الرقم الفريد الضروري لتفسير بيانات مؤمنة، والحصول على المفتاح عملية معقدة وكثيفة الاستخدام للموارد بالنسبة للمهاجم، ولكن بمساعدة تقنية، ويستعمل الهاكرز الأداة المكشوفة الوصول إلى بيانات محمية أثناء الاتصال دون أن يشعر المرسل والمستقبِل بذلك، وبإستعمال تقنية المكشوف يمكن للهاكرز أن يفك تشفير قاعدة البيانات ويعدّلها وأن يستعمل المفتاح المكشوف لحساب مفاتيح إضافية. هذا النوع من التهديدات يمكن مستخدمين غير مرغوب فيهم أو أصدقاء المهاجم من أن يحصلوا على الوصول إلى شبكات أخرى مؤمنة[19].

10.3 التنصت: يتم عند حدوث الاتصالات في شكل نص غير محمي وغير واضح مما يسمح للمتطفل من الوصول إلى قراءة وكتابة الطرود في قاعدة بيانات الشبكة، هذا ويقع تنصت على الشبكة عندما يحدث تطفل على الاتصالات، وإن قدرة المهاجم على التحكم في الشبكة تعد تحديا كبيرا تجاه المشاكل الأمنية التي يواجهها مدراء الشبكات في شركة ما، مثلا مجموعة المهاجمين

الذين يملكون أجهزة كمبيوتر محمولة ويتجولون بحثا عن شبكات من أجل الاتصال بها، وهم غالبا لا يلحقون أي ضرر وهذا بما أنهم متحمسون من أجل الوصول إلى فتح الشبكات المجانية ومشاطرتها مع الأصدقاء والزملاء، فمن دون التسيير المناسب وخدمات المصادقة القوية التي تقوم على أساس النزاهة والترميز يمكن قراءة وإعادة كتابة المعلومات من قبل المستخدمين غير المرغوب فيهم[20]، وهناك نوعان من التنصت[21]:

- **مراقبة الرسائل**: وفيه يهدف المتنصت الحصول على معلومات أو التقاط كلمات السر وقد يتم ذلك حديثاً بشكل آلي بمعنى وجود برامج متخصصة في البحث عن هذه الغايات.
- **إعادة إرسال الرسائل**: حيث يتم تخزين البيانات التي تحملها الرسائل أثناء إرسالها عبر الشبكات، ومن تم يعاد تمريرها إلى وجهتها المقصودة أصلاً وهذا النوع من التنصت يمكن كبحه عبر استخدام بروتوكول يمنع إعادة إرسال الحزم.

11.3 إهدار وقت العمل على الانترنت[22] (Cyber Loafing): وهذا النوع من التهديدات مرتبط بالسلوكيات السلبية للعاملين بمؤسسات البنية التحتية الحرجة وهو يهدد نوعا من سلوكيات الانحراف في العمل، ويرتبط باستخدام العاملين لتسهيلات تكنولوجيا المعلومات والاتصال الخاصة بالمؤسسة في أغراض شخصية بخلاف متطلبات انجاز العمل، واهم المشكلات الناتجة عن ذلك:

- إهدار الوقت وفقدان الإنتاجية والميزة التنافسية.
- إفشاء المعلومات السرية الحرجة وانتهاك خصوصية المعلومات.
- جلب المزيد من التهديدات مثل البرمجيات الضارة والبريد العشوائي وهجمات عرقلة الخدمة.
- الاستخدام غير الكفء وإهدار موارد تكنولوجيا المعلومات والاتصالات.

4. أهم الوسائل التقنية المعتمدة في أمن الأعمال الالكترونية

في ظل تهديدات ومخاطر أمن نظم المعلومات تسعى الكثير من المؤسسات لإيجاد السبل والوسائل الوقائية والإجرائية التي تمكنها من مواجهة التهديدات الأمنية لكي تتمكن من القيام بوظائف أمن المعلومات ويتزايد الاهتمام بحماية نظم المعلومات سعياً لتقليل التكاليف ولضمان استمرارية العمل وجودة المعلومات المقدمة وهو ما من شأنه تعزيز استقرار المؤسسات للقيام بدورها في تقديم الخدمات والتي أصبح جُلها يقدم بصورة آلية.

1.4 البرمجيات المضادة للاعتداءات الالكترونية: تعد البرمجيات المضادة للاعتداءات الالكترونية من وسائل الأمن الأكثر إنتشارا والأكثر معرفة من قبل مستخدمي الحاسبات والشبكات، وهي تعمل على البحث وتحطيم البرامج الخبيثة التي يمكن أن تتواجد بذاكرة الحاسب أو بأحد وسائط التخزين، وعلى منع تحميل هذه البرامج من خلال أحد أجهزته المحيطية للإدخال أو عبر الشبكة المرتبط بها، وتعمل كذلك على إيقاف ومنع أغلب الإعتداءات بإستعمال برمجيات وبرامج الجوسسة، والإعتداءات بإستعمال أسلوب اعتراض البيانات، وغيرها من الإعتداءات، ومن أهم البرمجيات نذكر منها[23]:

- برمجية Nettools: التي تسمح بالكشف عن نقاط ضعف نظام تشغيل الحاسب،
- برمجية Acunetix: التي تسمح بكشف نقاط ضعف متصفح الويب،
- برمجية N- Steath HTTPsecurity Scanner: التي تسمح بكشف نقاط ضعف شبكة الحاسبات،
- برمجية IOP Phcrack: التي تسمح بإختبار درجة قوة كلمات المرور المستخدمة بالشبكة،
- برمجية Spybot- Search. Destroy: التي تسمح بالقضاء على مختلف برامج الجوسسة،

- برمجية X-Netstat professional: التي تسمح بالكشف عن حدوث الإعتداء،
- برمجية Antisniffer: التي تسمح بإيقاف المعتدين بأسلوب اعتراض وتحليل البيانات،
- برمجية Steganos Intenet Anonyme: التي تسمح بالإبحار في الانترنت بشكل مخفي،
- برمجية Coffre-fort: التي تسمح بإنشاء حيز أمن بالحاسب لوضع البيانات الحساسة.

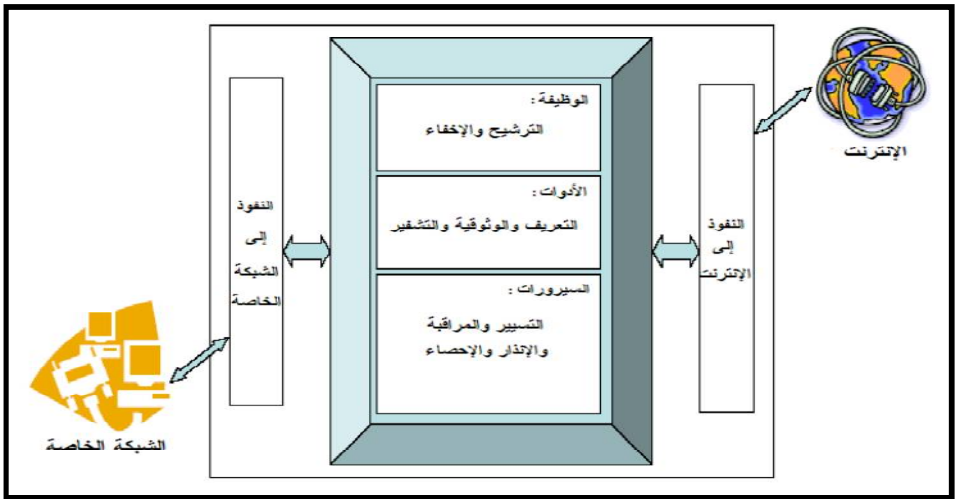
وبالإضافة إلى البرمجيات السابقة الذكر توجد برمجيات متكاملة للكشف عن البرامج الخبيثة والقضاء عليها، تدعي ببرمجيات أمن الانترنت ، ومن أبرز هذه البرمجيات نذكر البرمجية الروسية Kaspersky Internet Security التي تحتوي على كل من أدوات اكتشاف وتحطيم البرامج الخبيثة بالملفات، وأدوات اكتشاف وتحطيم البرامج الخبيثة عند الارتباط بالإنترنت، وأدوات اكتشاف وتحطيم البرامج الخبيثة على البريد الالكتروني، وكذلك أدوات اكتشاف الاحتيال عبر الانترنت، وأدوات اكتشاف المعتدين أو الهاكرز، وأدوات إيقاف البريد الالكتروني غير المرغوب فيه، مع إمكانية التحديث الآلي لقاعدة البرامج الخبيثة التي يمكن للبرمجية التعرف عليها.

2.4 التشفير: مصطلحا فك التشفير وعلم التعمية يستعمل أحدهما مكان الآخر، إلا أنه لغرض هذا البحث فإن علم التعمية يعّرف بأنه الفن أو العلم الذي موضوعه مبادئ ووسائل ومناهج جعل نص عادي غير واضح وتحويل الرسائل المشفرة إلى شكل مفهوم واضح، التشفير هو عملية تحويل نص عادي إلى نص مشفر، ويستعمل الترميز مرادفا للتشفير، لكنه أيضا ينطوي على فعل ترميز رسالة[24]، ويعرف Kessler[25] التشفير بأنه العلم الذي يحول المعلومة الواضحة إلى معلومة سرية غير قابلة للفهم، ويذكر هنا ضرورة التشفير حال الاتصال عبر وسائط غير موثوقة، وخصوصاً في حالة التراسل من خلال الانترنت، ويمكن تقسيم الشفرات إلى صنفين بحسب مفهوم إدخال المفتاح الذي يستعمله كل صنف: متناظر ولا متناظر. يستعمل التشفير المتناظر نفس المفتاح في التشفير وفي فك التشفير، وإن كان مختلفا بالإمكان يستخرج أحدهما من الآخر، حيث يستعمل إدخال المفتاح المتناظر يجب إرسال المفتاح إلى النهاية البعيدة، إدخال المفتاح المتناظر يسمى أيضا: تشفير المفتاح الخاص، وتستعمل الشفرة اللامتناظرة مفاتيح مختلفة في التشفير وفك التشفير، ومن غير الممكن من الناحية الحاسوبية استخراج مفتاح من مفتاح آخر، ويسمى هذا الشكل من التشفير بتعمية المفتاح العام[26]، وتعتمد آليات التشفير على المفاتيح أو كلمات السر، كلما كان المفتاح أطول كلما صعُب اختراقه، ومعيار تشفير البيانات واحد من أشهر لوغريتمات التشفير، ويعتمد على مفتاح طوله 56 رقما ثنائيا (بت)، وهو قابل للفك حاسوبيا، والمفاتيح الأقوى يمكن أن يكون طولها مئات البتات (الأرقام الثنائية)، وتوجد آليتان للتشفير (متناظر، لا متناظر) مفتاح خاص ومفتاح عام، ويستعمل المفتاح الخاص مفتاحا واحد لترميز وفك ترميز البيانات، أما المفتاح العام فيستعمل مفتاحا للترميز ومفتاحا آخر لفك رموز البيانات، يأتي اسم المفتاح العام من الخاصية الفريدة لهذا المفتاح أي أن أحد المفتاحين يمكن أن يتاح للعامة دون كشف خصوصية رسالة المفتاح الآخر، وتستخدم الشبكات الافتراضية الخاصة آليات التشفير من أجل تقديم نقل أمن عبر الشبكات العامة مثل الانترنت[27]، وفي دراسة لآليات الأمان التي تستخدمها المؤسسات الأسترالية بينت أن 47% من المستجوبين استعملوا شيئا من تشفير الملفات لحماية بياناتهم وأن 46% أشاروا إلى أنهم استعملوا تسجيل دخول أو جلسات مشفرة لضمان السرية، بالمقارنة مع الولايات المتحدة 60% من المؤسسات استعملت تسجيل دخول مشفر و58% استخدمت ملفات مشفرة[28].

3.4 الجدران النارية: جدار النار هو عبارة عن مكونات مادية (معدات وأجهزة)، وبرمجيات خاصة توضع بين الشبكة الداخلية للمؤسسة من جهة وبين الشبكات الخارجية، وهو يعمل على منع المستخدمين الخارجيين من التوغل في الشبكات الخاصة فهو نظام للحماية مزود ببرمجة خاصة تمنع الغرباء من اختراق الشبكات الخاصة، لذا فإنه يوضع هذا الجدار بأجهزته

وبرمجياته في مكان مناسب بين الشبكة الداخلية للمؤسسة والشبكات الخارجية بما في ذلك الانترنت، وقد صمم جدار النار بطريقة تؤمن له اعتراض كل حزمة رسائل تمر بين شبكتين وتفحص صفاتها ومن ثم رفض أي رسالة غير مخولة الدخول والاختراق[29]، كما هو مبين في الشكل التالي:

الشكل رقم 03: هيكلة الجدار المقاوم للنار.



المصدر: نوفيل حديد، تكنولوجيا الانترنت وتأهيل المؤسسة للاندماج في الاقتصاد العالمي – مع دراسة حالة المؤسسات الجزائرية– أطروحة مقدمة ضمن متطلبات نيل شهادة الدكتوراه دولة في العلوم التسيير غير منشورة، جامعة الجزائر، 2006-2007، ص: 188.

ويمكن تقسيم الجدران المقاومة للنار إلى نوعين أساسين هما[30]:

- **الجدران المقاومة للنار**: يمكن إستعمال هذا النوع من الجدران على الحاسبات المستقلة أو الحاسبات المرتبطة بالشبكة أو على الخوادم، ومن أشهر الجدران النارية نذكر: zone Alarm Pro وeSafe Desktop، و Blacklce Defender، وGardian بالإضافة إلى كل من Kaspersky Internet Security، و Norton Security Intenret، وMc Afee Personal Firewall.
- **الجدران المقاومة للنار**: تسمي كذلك بالعلب السوداء وهي تستعمل عادة على الخوادم وهي أكثر أمنا من الجدران البرمجية، لكونها غير معنية بنقاط ضعف نظام تشغيل الحاسب أو بمختلف ثغراته، ومن أشهر الجدران المادية نذكر WathGuard، و WatchGuard SOHO.

قبل أن ننهي حديثنا عن أمن شبكات المعلومات والمخاطر التي تتهددها إلى وضع متطلبات حماية البنية التحتية المعلوماتية إلى تحقيق ثلاث أهداف إستراتجية وهي[31]:

- منع الهجمات الالكترونية ضد البنية التحتية الحرجة (المادية والمعلوماتية).
- تخفيض نقاط الضعف والثغرات الأمنية الوطنية (في البنية التحتية الوطنية).
- تقليص التخريب والتدمير إلى ادني درجة واستعاد الوضع السابق للهجمات الالكترونية التي تحدث.

كما نورد بعض الإجراءات العامة التي يمكن وضعها في الاعتبار كوسائل احترازية يمكن تطبيقها والتي يمكن التعبير عنها بأنها من متطلبات أمن الشبكة بصفة عامة وهي كالتالي:

- **تحديد سياسات العمل في شبكات المعلومات:** بأن يكون واضحاً تمام الوضوح ما هو المسموح به والممنوع فيما يتعلق بأمن المعلومات على الشبكة.
- **توفير آليات تنفيذ سياسات العمل:** بأن يكون معروفاً كيفية تنفيذ هذه السياسات وما هي العقوبات التي ستوقع في حالة المخالفة.
- **العنصر البشري:** بأن يتولى إدارة وتشغيل شبكات المعلومات عناصر بشرية مدربة ومؤهلة للتعامل مع هذه التكنولوجيا وألا يترك المجال للهواة للعبث بمثل هذه المقدرات الثمينة وخاصة في الأماكن الحكومية والحيوية على مستوى الدول.
- **تغيير الأوضاع الأصلية لمعدات الشبكات:** وذلك بأن يتم كل فترة تغيير الأوضاع الأصلية للمعدات Hardware، والبرامج Software الخاصة بشبكات المعلومات كإجراء احترازي كل فترة لمنع الاختراقات الخارجية.
- **المراقبة:** يجب أن يكون هناك نوع من المراقبة والمتابعة لأنشطة المعلومات على الشبكة بشكل دقيق ودائم وذلك بهدف إكتشاف أي أنشطة مشبوهة أو حركات غير طبيعية ضمن نطاق الشبكة وتفادي تفاقم الأوضاع.
- **حسن إختيار مواقع نقاط الشبكة:** فيجب أن يتم التدقيق جيداً عند اختيار نقاط الاتصال بشبكات المعلومات، وأن تكون هذه النقاط في مواقع جيدة ومؤمنة ومحمية.
- **بروتوكولات التحقق والتشفير:** يجب أن يتم تشغيل بروتوكولات التحقق من الهوية وأنظمة تشفير البيانات لتأمين المعلومات على الشبكة، وأن يتم اختيار البرامج ذات السمعة العالمية في هذا الإطار.

5. خلاصة:

يشهد عالم اليوم تغيير اً مستمًرا في بيئة الأعمال، وتطويرا لا يتوقف على صعيد إنجاز المهام اليومية والتعامل مع جمهور العملاء في مختلف القطاعات، ولقد أصبحت تكنولوجيا المعلومات ضرورة من ضرورات عصرنا الحالي وأداة من أدوات العمل الرئيسية، بل وأصبحت أداة إستراتيجية تسهل الوصول إلى الميزة التنافسية الدائمة، ونتيجة لهذه الطفرة الكبيرة التي حدثت في وسائل الاتصالات وشبكات المعلومات والدخول في عصر العولمة والانترنت، ظهرت مخاطر وتهديدات جديدة في ساحة الأعمال وهو ما يستدعي أخذ كافة الوسائل المتاحة أو الممكنة لتعزيز أمن نظم المعلومات وحمايتها في ظل توجهنا نحو اقتصاد قائم على الاتصال والبيانات الكبيرة وانترنت الأشياء. فالحكومات والشركات الكبيرة وحتى الشركات الصغيرة الحديثة الإنشاء أصبحت غير قادرة على تحمل تكلفة الاستثمار بالحلول الغير مجدية لكشف ومعالجة تحديات أمن المعلومات، كما أصبح من الضروري بالنسبة لها أن تعي تأثير أمن المعلومات على استراتيجياتها واستدامتها على المدى الطويل.

6. الهوامش والإحالات:

[1]Ponemon Institute, Research Report, (October 2013): Cost of Cyber Crime Study:United States, Sponsored by HP Enterprise Security Independently conducted by Ponemon Institute LLC, p: 1

[2]Eric Filiol, (2009): « Les virus informatiques : théorie, pratique et application », 2eme édition, Springer, Paris, p: 111.

[3]U.S. Government, (2013): Legal Information Institute, Title 44, Chapter 35, Subchapter 111, 3542, Cornell University Law School. www.law.cornell.edu/uscode/44/3542.html (02 -12-2016).

[4]Forouzan, Behrouz A, (2008): Introduction to cryptography and network security, Mcgraw-Hill Education - Europe, Category: Books, ISBN: 9780072870220, p: 3.

[5]http://technet.microsoft.com/en-us/library/cc959354.aspx (05-12-2016).

[6] عبير فاروق محمود عبد الرحيم تمام، دور الاقتصاد الرقمي في دعم التنمية مع إشارة خاصة للاقتصاد المصري، رسالة مقدمة للحصول على درجة دكتوراه الفلسفة في الاقتصاد غير منشورة، جامعة عين شمس، مصر، 2009، ص: 91.

[7]James A , Senn, (2004): Information Technology – Principles, Practices, Opporunities, Pearson Prentice, Third Edition, p: 578.

[8] محمد دباس الحميد وماركو ابراهيم، حماية أنظمة المعلومات، الطبعة الأولى، دار الحامد، الأردن، 2007، ص:167.

[9]Turban, leidner, MC Lean, and Wetherbe, (2006): Information Technology for management-Transforming organizations in the Digtal Economy, John Wiley Sons Inc, p: 650.

[10]Kaspersky, (2012): Research Report, Global IT Security Risks, p: 6.

[11]Computer Security Institute, (2003): Fourth annual CSI/FBI computer crime and security survey, p: 89.

[12]http://technet.microsoft.com/en-us/library/cc959354.aspx(11-12-2016).

[13]Cisco systems, (2001): inc: (Indiana, Cisco press, Cisco networking academy program, first year companion guide 2nd ed, p: 123.

[14]James Carpent, Ray Hunt, (2006): Tighting the net : A review of current and next generation spam filtering tools, Computers,(Vol. 25. 8), p: 566.

[15]Casey, Eoghan, (October2001): 'Handbook of Computer Crime Investigation: Forensic Tools &Technology', Academic Press, p: 136.

[16]Willam Roberds, Stacy L- Schreft, (2009): Data breaches and identity, Journal of Monetary Economies, (Vol. 56. No. 7), p: 918.

[17]Computer Security Institute, op .cit, p: 91.

[18] نوفيل حديد، كربيط حنان، أمن المعلومات ودوره في مواجهة الإعتداءات الالكترونية على نظام معلومات المؤسسة، مجلة علمية دورية محكمة تصدر عن مخبر إدارة التغيير في المؤسسة الجزائرية، العدد:03، جامعة الجزائر،2014، ص:191.

[19]http://technet.microsoft.com/en-us/library/cc959354.aspx(12-12-2016).

[20]Wi-Fi Alliance, March (2005): Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise. Wi-Fi® is a registered trademark of the Wi-Fi Alliance, p: 26.

[21]Garfinkel,S.,Spafford,G.,Schwartz,A, (2003): Practical UNIX and Internet Security, Practical Series, O'Reilly Media, p: 253.

[22]Pablo Zoghbi- Manrique Lara, (2009): In equity, conflict and complainee dilemma as cases of cyber loafing, International Journal of Conflict Management, (Vol.2, No.2) , p: 188.

[23] نوفيل حديد، تكنولوجيا الانترنت وتأهيل المؤسسة للاندماج في الاقتصاد العالمي- مع دراسة حالة المؤسسات الجزائرية- أطروحة مقدمة ضمن متطلبات نيل شهادة الدكتوراه دولة في العلوم التسيير غير منشورة، جامعة الجزائر، 2006-2007، ص ص: 186-187.

[24]McClure, S., J. Scambray & G. Kurtz, (2005): Hacking Exposed: Network Security Secrets and Solutions. Berkeley: Osborne Press, p: 31.

[25]http://www.garykessler.net/library/crypto.html (23-12-2016).

[26]Khadraoui, D., and Herrman, F, (2007): Advances in Enterprise Information Technology Security – Illustrated Edition, Premier Reference Source, p: 54.

[27]Bejtlich, R., (2004): The Tao of Network Security Monitoring and Extrusion Detection, Addison-Wesley Professional, p: 141.

[28]Power, R, (2002): Tangled Web – Tales of Digital Crime From the Shadows of Cyberspace, Que, Indianapolis, p: 256.

[29] سهام عبد الكريم، دور تكنولوجيا المعلومات في تأهيل المؤسسات الصغيرة والمتوسطة دراسة عينة من المؤسسات (نادي المقاولين والصناعين لمتيجة، اطروحة الدكتوراه في العلوم التسيير غير منشورة، جامعة الجزائر 03، 2012-2013، ص: 21.

[30] نوفيل حديد، مرجع سابق، ص: 188.

[31]Eugene, Nickolov, (2005): CRITICAL Information Infrastusture Protection : analysis, evaluation, Information Security : An International Journal.(Vol.17), p: 106.