تهديدات أمن المعلومات وسبل التصدي لها

Information Security Threats And Methods Of Protection

ط.د. فيلالي أسماء
جامعة أبو بكر بلقايد، تلمسان، الجزائر
filaliasma@outlook.fr

أ.د. شليل عبد اللطيف
جامعة أبو بكر بلقايد، تلمسان، الجزائر
Chelil.abdellatif@gmail.com

تاريخ الاستلام: 2018/09/07 تاريخ القبول: 2019/02/08

الملخص:

لقد شهد هذا العصر انفجار معلوماتي هائل جعل المؤسسات مهما كان حجمها معرضة لمنافسة معقدة ومتزايدة، ومواجهة حادة مع التهديدات الناجمة عن التغير المستمر لبيئتها، ومن بين التهديدات التي تطال المعلومات وأنظمتها نجد التهديدات الطبيعية الناتجة عن الكوارث الطبيعية، والتهديدات البشرية سواء الناتجة عن خطأ أو الناتجة عن اعتداء إما بزرع البرامج الضارة مثل الفيروسات والديدان...أو عن طريق القرصنة المعلوماتية كالتصنت ورفض الخدمة....إضافة إلى التهديدات التقنية أو الناتجة عن ثغرات أمنية وهذا ما يستدعي تكثيف الجهود وتسخير كل الوسائل المتاحة والممكنة من اجل تعزيز امن المؤسسة، بتطبيق كل أنواع الحماية من حماية برمجية إلى حماية مادية وبشرية إلى حماية قانونية.

الكلمات المفتاحية: أمن المعلومات، التهديدات، الثغرات، حماية أنظمة المعلومات، القرصنة المعلوماتية.

Abstract:

This era has witnessed massive explosion in information subjecting both small and big businesses to a more increasing and complex competition and a strong confrontation to threats resulting from the ever increasing change of their environment. Among the threats facing information and its systems: natural threats due to natural disasters and human threats owing to mistakes or external attack either by planting malware , software and worms …or by pirating information such as phone tapping or service denial ..in addition to technical threats. This requires intensifying efforts and exploiting all the possible and available means to reinforce the company security by applying all sorts of protective measures: software, physical and human protection via judicial protection.

Key Words: Information Security, Threats, Information System Protection, Spyware, Protection Of Information Systems.
JEL Classification: D81, D83.

* مرسل المقال: فيلالي أسماء (filaliasma@outlook.fr).

المقدمة:

لقد واجهت الإدارة في العصر الحديث حالة من التحدي نتيجة الثورة العلمية أو بمصطلح أكثر دقة الثورة المعلوماتية، فالتطورات الحديثة في تقنية المعلومات جعلت من عملية تداول المعلومات وانتقالها أمرا سهلا وسريعا وفي متناول الجميع، ما جعلها عرضة للخطر، لهذا هي دائما بحاجة إلى حماية هاته المعلومات خاصة الإستراتيجية منها والحساسة، وهذا ما يستدعي تكثيف الجهود وتسخير كل الوسائل المتاحة والممكنة من اجل تعزيز امن المؤسسة ،و من هنا اشتدّ الانتباه إلى ضرورة وأهمية حمايتها والحفاظ عليها ونتيجة لجهود الباحثين والمتخصصين في هذا المجال ظهر مصطلح أمن المعلومات.

فأمن هو تحقيق حماية لكل الممتلكات المادية منها كالأجهزة والبنايات، وغير المادية كصورة المؤسسة وأنظمتها المعلوماتية وبالأخص المعلومات الإستراتيجية والحساسة، والتي تعتبر ثروة حقيقية في ظل اقتصاد المعرفة، فالتهديدات قد تطال إما توفر المعلومة أو سلامتها أو سريتها وأمنها.

إشكالية الدراسة:

إن المؤسسة مهما كان نوعها أو حجمها تتعرض إلى تهديدات تمس أمنها وهذا ما يدفع بنا إلى طرح الإشكالية التالية: **ما هي التهديدات التي تتعرض لها أنظمة معلومات المؤسسة؟و ما هي سبل التصدي لها ؟**

وعلى ضوء هذه الإشكالية يمكن طرح التساؤلات التالية:

- ما المقصود بأمن نظم المعلومات؟
- ما هي التهديدات التي تفرضها البيئة المحيطة ؟
- ما هي طرق الحماية الممكن تطبيقها ؟

ومن خلال هذه الورقة البحثية سنحاول الإجابة على هذه الإشكالية من خلال التطرق ل :

- مفاهيم حول أمن المعلومات وأنظمتها .
- التهديدات التي تتعرض لها المعلومات وأنظمة المعلومات.
- طرق الحماية الممكنة لتفادي التهديدات .

1. مفاهيم حول أمن المعلومات وأنظمتها

1.1. مفهوم أمن المعلومات

- عرف Whitman et Mattod أمن المعلومات في كتابهما **مبادئ أمن المعلومات** بأنه " الحفاظ على سرية وتوفر وسلامة المعلومات كأصل في مراحل المعالجة والحفظ والنقل، ويتحقق ذلك عبر التطبيق الفعلي للسياسات الأمنية ومن خلال تعزيز الوعي والتعلم والتدريب. (Whitman & Mattod, 2011)ويرى كلاهما أن تحقيق ادارة أمن نظم المعلومات يشمل المكونات التالية:

- الأمن المادي: بما يشمله من مصادر وممتلكات ومباني لمنع الوصول غير المشروع.

- أمن الأفراد: لحماية الافراد والمجموعات الذين لهم حق الوصول للمعلومات.
- أمن العمليات: لحماية الأنشطة والعمليات التي يقوم بها المخولون.
- أمن الاتصالات: لحماية الوسائط والتكنولوجيا المستخدمة والمحتوى.
- أمن الشبكات: لحماية مكونات الشبكة والتراسل والمحتويات.
- أمن البيانات: لحماية سرية وسلامة وتوافر المعلومات.

من خلال هذا التعريف يتضح لنا جليا أن أمن المعلومات ما هو إلا مصطلح يضم في محتواه أمن عام فحماية المعلومات تكون من خلال الأمن المادي كالأجهزة التي تضم المعلومات وأمن الأفراد الذين يملكون المعلومات، وكل العناصر ذات علاقة بالمعلومات.

– كما يعرف أمن المعلومات أنه " مجموعة من الاجراءات الادارية والفنية التي صممت لضمان حماية الأجهزة وملحقاتها، والبرامج والبيانات من السرقة أو التوقف أو التلف المتعمد أو غير المتعمد، أو التخريب أو التبديل أو مجرد الإطلاع دون تصريح بالاستخدام، وحماية شبكة المعلومات الداخلية والاتصالات الخارجية من الاختراق أو التعطيل المتعمد أو غير المتعمد "(الشدي، 2000، ص ص 82-83)

– و عرفه مجمع اللغة العربية في معجم الحاسبات أنه " حماية المعلومات من الكشف أو الاستنساخ أو التدمير من قبل أشخاص غير مصرح لهم سواء كان عرضا أو عمدا "(معجم الحاسبات، 1995) هذا التعريف ركز على حماية المعلومات من الأشخاص غير المصرح لهم بالإطلاع.

– وبالنظر إلى أمن المعلومات من عدة زوايا، فيمكن تعريفه على هذا الأساس:

–من زاوية أكاديمية (علمية): هو العلم الذي يبحث في نظريات واستراتيجيات وسياسات توفير الحماية للمعلومات من المخاطر التي تهددها.

–من زاوية تقنية(عملية):هو مجموعة الوسائل والتدابير والاجراءات التي يجب توفيرها لتأمين حماية المعلومات من المخاطر المتأتية سواء من البيئة الداخلية أو الخارجية.

–من زاوية قانونية: هو محل دراسات وتدابير حماية سرية وسلامة المحتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها واستغلال نظمها في ارتكاب الجريمة(بيهان، 2007)

وعلى ضوء التعريفات السابقة يمكن القول أن أمن المعلومات هو كل السياسات والإجراءات المطبقة بهدف حماية المعلومات عن طريق توفير الأمن لكل المكونات المادية من محلات وأجهزة والمكونات التقنية كالبرمجيات والشبكات والاتصالات وكل التكنولوجيات المستعملة في تداول المعلومات، وتوعية العنصر البشري.

2.1 . عناصر أمن المعلومات

أ. **السرية (Confidentiality)**: تعني ضمان حفظ المعلومات المخزنة أو المنقولة ،و عدم الإطلاع عليها أو استخدامها إلا بموجب إذن ،حيث أن النظام الآمن هو الذي يضمن سرية وخصوصية البيانات المخزنة فيه.

ب. التكاملية والسلامة (Integrity):هي بصفة عامة ضمان سلامة محتوى المعلومات، والتأكد أن هاته المعلومات لم تتعرض لأي عملية حذف أو تخريب أو اتلاف كلي أو جزئي سواء بصفة متعمدة أو غير متعمدة .

ج. التوفر والإتاحة (Availability): ونعني به تمكين المستخدم (إنسان أو نظام حاسوب) الذي له حق التعامل مع المعلومات من ذلك بدون التدخل أو الإعاقة في أداء تلك المهمة، ووصول المعلومات في الشكل المطلوب.

2. تهديدات أمن المعلومات

التهديد هو كل تصرف يمكن أن يؤثر سلبا على عناصر الأمن.

1.2. مصادر التهديد

أ. التهديدات الطبيعية: هي كل التهديدات الخارجة عن الإرادة ومنها:

أ.1. الكوارث الطبيعية: مثل الزلازل والفيضانات والنيران، إضافة إلى درجة الحرارة العالية والرطوبة العالية التي تلحق الضرر بالحاسوب والأجهزة الالكترونية.

أ.2 التهديدات التقنية: هي المشاكل التي تؤدي إلى توقف الأعمال لفترات ،ما يسبب خسائر للمؤسسات كانقطاع التيار الكهربائي،الانترنت،حدوث أعطال في مكونات نظم المعلومات.

ب. التهديدات البشرية: وتتمثل في مصادر خارجية تصدر من أعوان خارجية (المنافسين ،الحكومات أو المصالح الخارجية ،المنظمات الإجرامية ،جماعات الضغط ،المجتمع..)،أو داخلية(أجراء غير راضين أو أجراء قدماء، متدربين) (Delbecque & Fayol. 2012, pp 89-90)

وحتى نهاية القرن العشرين مصدر الجرائم المعلوماتية الأكثر خطورة كانت ذات مصدر داخلي صادرة من العمال نظرا لامتلاكهم المعارف، وقدرتهم في الوصول إلى الأنظمة .(Laudon & Laudon,2006, p355)

ومقارنة بين حجم الخطر الداخلي وبين حجم الخطر الخارجي نذكر بعض الاحصائيات:

- وفقا لوكالة FBI تشكل التهديدات الداخلية من 60% إلى 80% من التهديدات المخبر عنها.
- وحسب دراسة قامت بها Gartner Group على المخطط الأوروبي سنة 1997،ذكرت المنظمات أن مشكل الأمن هو بنسبة 47% من الأعوان الداخليين ويعتبر العمال القدماء مسؤولين بنسبة 10% من الحوادث، أما الخارجيين فهم مسؤولين بنسبة 39%. (Godart ,2005, p23)
- وحسب دراسة أجريت سنة 2003 على 408 خبير معلوماتي يقولون أن 94% من الأدوات المعلوماتية المسؤولة تعرضت لمشكل أمني من مصدر داخلي قام به المستخدمون. (Godart ,2005, p23)
- كما كشفت دراسة أجرتها الأمم المتحدة عام 2005 أن 37% من جرائم الاختراق والتعدي داخلي، وأن 23% يرجع إلى مصادر خارجية، وبلغ حجم الخسائر الاقتصادية لهذه الجرائم عام 2004 فقط حوالي 3.5 مليار دولار، كما كشفت الدراسة أن حالات الاختراق بصفة خاصة كإحدى الجرائم المعلوماتية التي وقعت على

أجهزة الحكومة الأمريكية لعام 2004 بلغت 354000 حالة اختراق، 64% منها ناجحة ولم يكتشف سوى 4% منها.(الرشيدي علي بن ضبيان،، 2000 ص 12.)

- و بخصوص تحصين أنظمة المعلومات فتكون الجهود المبذولة والمسخرة في التحصين ضد التهديد الخارجي على حساب الاستعداد ضد التهديد الداخلي، في حين هذا الأخير غالبا ما يحدث دمارا باهظ التكاليف. فحسب تقديرات معهد أمن الحاسوب فإن معدل تكاليف الهجوم الداخلي هو 2.7 مليون دولار للهجوم الواحد، بينما لا يزيد معدل الهجوم الخارجي الواحد عن 57 ألف دولار
(http://www.sans.org/rr/papers/60/475.pdf.)

– هذه الدراسات والإحصائيات أثبتت بالإجماع أن التهديد الأكبر الذي تتعرض له المؤسسة وأنظمتها المعلوماتية هو من الداخل وبنسب كبيرة جدا مقارنة بالتهديد الخارجي.

2.2 . أنواع التهديدات على المعلومات ونظم المعلومات

أ. **التهديدات الناتجة عن اعتداء:** ومن تقنيات الاعتداء نجد :

أ.1. البرامج الضارة(الخبيثة):وهي كل برنامج يدخل في النظام ويكون عمله ضارا،منها:

– **الفيروسات:** التعريف الذي يمثل المرجعية في عالم الأمن هو تعريف « Fred Cohen » الذي عرف الفيروس على أنه: " برنامج له القدرة على إصابة برامج أخرى عن طريق تعديلهم بطريقة تجعلهم يحتوون على صورة منه" (Lafitte, 2003, p90) وكان Fred Cohen أول من تداول أو أخرج مصطلح "الفيروس المعلوماتي" سنة 1984.

الفيروس برنامج خبيث تم تصميمه من قبل أحد المبرمجين لتحقيق بعض الأهداف وحسب هذه الأهداف تكون النتائج، قد تكون غير مضرة كإظهار بعض الإعلانات ،قد تكون خطيرة نوعا ما كتعديل جزء من البرامج ،و أغلبها يكون مدمر كتعطيل وتدمير البرامج والأجهزة كلية ،و من سمات الفيروس قدرته على ربط نفسه بالبرامج ونسخ نفسه بنفسه دون علم المستخدم إضافة إلى قدرته على التخفي والانتشار السريع .

– **الديدان Vers**: الديدان عبارة عن برامج مستقلة تنتقل من حاسب لآخر داخل الشبكة دون الحاجة لتدخلات بشرية، وتنتشر بسرعة أكبر من الفيروس، ويمكن أن تخفي معطيات وبرامج واتلافها، وإعاقة عمل شبكة معلوماتية ،(Laudon & Laudon, 2006, p352) فالديدان المعلوماتية تستقر في ذاكرة أنظمة المعلومات بنفس الطريقة التي تستقر فيها الدودة البيولوجية في تفاحة، وعلى عكس الفيروس، فهي قادرة على نسخ نفسها بدون تدخلات داخلية أو خارجية.

– **حصان طراودة Chevaux de Troie**: يعرف حصان طراودة على أنه: " رمز خبيث يختفي داخل برنامج، مُظهرا بذلك براءته عن طريق تمثله في لعبة صغيرة أو بطاقة رغبات أو برنامج مشاهدة صور من أجل أن ينفذ لاحقا عمليات غير شرعية "(Godart ,2005, pp 65-66)

فهو " برنامج غير خطير في الظاهر، ولكن تصرفاته غير متوقعة، ليس فيروس لأنه لا يتكاثر، ولكن يمكن أن يمرر فيروسات ورموز خبيثة أخرى من أجل أن يضمن دخوله في النظام المعلوماتي " ,Laudon & Laudon,2006) p355).

– **القنابل المنطقية Bombe logique**: القنبلة برنامج متخفي في انتظار حدث معين محدد من قبل المبرمج، ويُشغَّل هذا البرنامج الخبيث عندما يحدث الحدث، هذا الرمز الخبيث ينتظر عموما تاريخ معين من أجل أن يباشر العمل (Menaces sur les systémes informatique « Guide N 65 »2006 , p15)

أ.2. القرصنة المعلوماتية (التجسس على أنظمة المعلومات): القرصنة تعمل على كشف نقاط ضعف نظم حماية الأنظمة المعلوماتية، وغالبا ما يتم استغلال مختلف وظائف الانترنت التي تحوله إلى نظام مفتوح سهل الاختراق ،و عليه هذا النوع من تقنيات الاعتداء يتمثل في محاولة اقتحام أنظمة المعلومات والحصول على المعلومات السرية بأي طريقة، وسنقوم بذكر أكثر الطرق انتشارا .

– **التصنت L'Ecoute** :التصنت يكمن في التموقع على شبكة معلوماتية أو شبكة التواصل عن بعد ،و من ثم تحليل وتخزين المعلومات العابرة ،و ترجمة التآمرات وكل ما يدور داخل الشبكة المعلوماتية.

إذ أنه وعلى مستوى الاتصال بالشبكة أو الانترنت العادية 99.9% من المعلومات التي تدور ليست مشفرة، ويمكن اعتراضها من قبل أي أحد. .(Royer ,2004 , p23)

ومن أكثر البروتوكولات عرضة للتصنت بروتوكول(TCP/IP**)،ومن الأدوات المستخدمة لتنفيذ التصنت برامج تحليل الشبكات وبروتوكولاتها كبرنامج " Sniffer "الذي يعرف على أنه برنامج التصنت الالكتروني الذي يراقب المعلومة المنقولة داخل الشبكة" . .(Laudon et Laudon,2006, p354)ويسمح بالتصنت على حركة الشبكة المعلوماتية التي تتصل مباشرة بالحاسب، ومن أولوياته البحث عن تحديد الحزم التي تضم كلمات login أو password. (Léopold & Lhoste, 2007, p53)

– **سرقة الهوية l'usurpation d'identité**: تكمن في انتحال هوية شخص آخر والاستفادة من امتيازاته عن طريق اغتصاب هويته والاستيلاء على العديد من العناصر الخاصة به(بصمة ،صوت ،بطاقة تعريف ،بطاقة ائتمان ،شريحة، كلمة سر، تاريخ ميلاد...)

– **رفض الخدمة** :هذه الهجمة حتى وإن كان ظاهرها غير مخيف إلا أن تأثيرها كبير:

– هي نشاط خبيث يترجم بانشغال أو عدم اتاحة مؤقت أو دائم لعدة مكونات نظام الاتصال عن بعد (Lafitte, 2003, p88)

– هجمة رفض الخدمة هي تلك التي تعرقل وتمنع خدمة تطبيق ما وجعلها أحيانا غير مفيدة للمستعملين الشرعيين، باختصار هجمة رفض الخدمة تعمل على ازعاج الضحية، ولكن أيضا يمكن أن تتسبب في خسائر كبرى (Gallagher., Jeffries. & Landauer, 2007, p375)

– **التزوير أو التعديل**: تزييف وتعديل المعطيات خلال الارسال بتدخل خبيث يحدث مشكل التكامل، فالتكامل المضمون عن طريق بروتوكولات النقل (TCPمثلا) تضمن أن يكون جريان المعطيات المستقبلة مماثلة تماما

لجريان المعطيات المرسلة (Vaucamps, 2010, p14) ، وبالتدخل بينهما وتعديل الرسائل المرسلة لا تكون هذه الأخيرة نفسها هي المستقبلة، أما التعديل في البرامج يجعلها تؤدي عملها بطريقة مختلفة تلبية لمصالح المهاجم .

أ. **3. التهديدات المادية:** التهديدات التي تمس الأجهزة المعلوماتية تعني تهديد أمن المعلومة التي تحتويها ومنها:

– **السرقة:** تستهدف كل ما يتعلق بأنظمة المعلومات ،.فخسارة سرقة جهاز مثلا تكمن في ثمنه ،اضافة الى قيمة المعلومات التي يحملها الجهاز والتكاليف المتكبدة في خسارتها

– **الوصول والتدمير المادي:** مجرد الوصول إلى الأجهزة المعلوماتية فهذا بحد ذاته خطر أمني، كما أنه يمكن للمهاجم أن يدمر إراديا التجهيزات وتخريبها.

– **الهندسة الاجتماعية:**هذه التقنية تعتمد على التلاعب بالأفراد للتمكن من آليات الأمن باعتبار أن العامل البشري هو الحلقة الضعيفة في نظام المعلومات مستغلين بذلك سذاجة الشخص (Atelin, 2009 , p 314).

فالهندسة الاجتماعية هي من أسهل الطرق للحصول على المعلومات باعتمادها على وسائل بسيطة وحيل وخداع، ومن بين أساليبها: التفتيش في النفايات، التظاهر بالسلطة،خداع شخص واستغلال ضعفه، انتحال شخصية....

ب. **التهديدات الناتجة عن ثغرات أمنية:** تعتبر الثغرة الأمنية عبارة عن فجوة أو ضعف على مستوى نظام المعلومات، ومن الممكن استغلالها من طرف عناصر مهددة باستعمال مختلف طرق الهجوم. وعليه الثغرة الأمنية هي عبارة عن ضعف أو خطأ في نظام معين أو طريقة حماية معينة يتم استغلالها من قبل المهاجم لإحداث أضرار مختلفة، وتكون الثغرة الأمنية على ثلاث مستويات: الثغرات الأمنية على المستوى التنظيمي (الادارة)، الثغرات الأمنية على المستوى المادي، الثغرات الأمنية على المستوى التكنولوجي.

3. طرق تحقيق أمن نظم المعلومات

1.3 . **الحماية البرمجية للمعلومات وأنظمة المعلومات:** الحماية البرمجية تتمثل في استخدام كل البرامج المتاحة والتي توفر حماية للمعلومات المنتقلة عبر الشبكات أو المخزنة في الحواسيب.

أ. **الجدار الناري:** ويمكن تعريف الجدار الناري على أنه: "كل آلة موضوعة في شبكة معلوماتية وقادرة على تحقيق غربلة على التواصلات الداخلة والخارجة "(Léopold & Lhoste, 2007, p85)

ويعرف أيضا أنه:"جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب ،و يكون أداة مخصصة أو برنامج على جهاز حاسوب آخر الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة ويرفض أو يقرر أحقية المرور ضمن قواعد معينة ". (حسين ،2011 ص 192)

أما بالنسبة لأشكال الجدار الناري، فهي تأتي على نوعين: .(Royer ,2004 , p61)

– برامج: وهنا يكون الجدار الناري عبارة عن برنامج يتم تنزيله على الحاسب.

– أجهزة: وهو عبارة عن علبة أو صندوق مزود بواصلين اثرنت، هاته العلبة تضم في نفس الوقت حاسب وبرنامج جدار ناري .

ب. برامج مكافحة الفيروسات Anti virus : برنامج مكافحة الفيروس يتحقق من الأقراص والأنظمة من أجل تحديد تواجد فيروسات معلوماتية، ويستطيع عموما تنظيف المنطقة المصابة، ومن أجل أن يبقى البرنامج فعال يجب أن يُحدّث باستمرار. (Laudon & Laudon, 2006, p373)

– التشفير Chiffrement : " هو مجموع التقنيات التي تهدف إلى تحويل بفعل اتفاقيات سرية، معلومات أو إشارات واضحة إلى معلومات أو إشارات غير واضحة من أجل تحقيق الفرضية المعاكسة عن طريق وسائل مادية أو برامج متخصصة لذلك ".(Léopold & Lhoste, 2007, p72) .

– "هو الاعتماد على خوارزمية لتحويل المعطيات الواضحة إلى معطيات مشفرة من أجل جعلها غير واضحة لشخص دخيل (Pelletier & Cuenot ,2003 , p 35) ،و الهدف من التشفير هو جعل كل الملفات الرقمية الموجودة على التحاميل غير صالحة الاستعمال لمن لا يملك مفتاح الرمز.

وعليه فإن التشفير عبارة عن استخدام تقنيات أو برامج عملها هو تغيير مظهر المعلومات من معلومات واضحة يسهل فهمها إلى معلومات سرية يصعب فهمها، إعتمادا على :

– خوارزمية التشفير:هي الصيغة الرياضية المطبقة على المعلومات المراد تشفيرها.

– المفتاح التشفيري: وهو السر أو الأداة المستعملة في تشفير أو فك شفرة المحتوى.

ت. مراقبة الدخول وأنظمة كشف التدخل:

ث.1. مراقبة الدخول (Contrôle d'accès) :مراقبة الدخول هي كل السياسات والاجراءات المتخذة من قبل مؤسسة من أجل ايقاف أو إعاقة الدخول للأنظمة من قبل أشخاص ممنوعين، والدخول إلى النظام يتطلب التعريف بالهوية + التحقق من الهوية.

ث.2. أنظمة كشف التدخل Intrusion Detection Systems IDS : أنظمة كشف التدخل هي عبارة عن أدوات مراقبة مستمرة موضوعة في أماكن أو نقاط الدخول الأكثر حساسية لشبكات المؤسسة من أجل كشف التدخلات، ومن ثم يطلق النظام إنذار في وقت حقيقي في حال حدث مريب أو غير عادي.

ث.الشبكة الافتراضية الخاصة Virtuel Private Network VPN: هي تكنولوجيا حديثة يتم من خلالها حماية تبادل المعطيات بين موقعين متباعدين على الأقل، ضامنة بذلك هويات المرسل والمستقبل، إضافة إلى ضمان عدم انتهاك المعطيات وتكاملها وتأكيد عملية ارسالها واستقبالهافشبكة VPN تشفر حركة مرور الشبكة الحساسة ،و عملها يتم من خلال خادم VPN الذي يمثل مقر المراقبة داخل المؤسسة .

ج. التحديثات: نجد نوعين من التحديثات :التحديث الآلي عن طريق قيام البرنامج المثبت في الحاسوب الاتصال بالشركة الأم للتحقق من وجود أي تحديثات، فإن وُجد أي منها بادر البرنامج بتنبيه المستخدم إلى ذلك، ويتطلب هذا اتصال الحاسوب بالانترنت، أما الثاني فهو التحديث اليدوي والذي يكون بمبادرة من المستخدم الذي عليه الذهاب إلى الموقع الالكتروني للشركة المصنعة للبرامج ويقوم بتحميل التحديثات اللازمة. (الغثبر والقحطاني، 2009، ص ص 99-100)

2.3. الحماية المادية لممتلكات المؤسسة المادية (الأمن المادي)

تحقيق الأمن المعلوماتي لا يكون بحماية المعلومات داخل الحواسب فقط، بل من الضروري تحقيق الأمن الخارجي والمادي للمنظمة وموقعها وتجهيزاتها.

أ. **أمن موقع المنظمة:** هو تحقيق الأمن المادي لموقع المنظمة والسيطرة الخارجية للبناية وحمايتها من كل تدخل طبيعي أو متعمد من خلال عدة إجراءات :

- الاختيار الأمثل لموقع المنظمة.
- تحديد نطاق المؤسسة وتقسيم المواقع الواجب حمايتها .
- تشييد آليات منع الدخول عن طريق: تركيب سياج أو سور ملائم للمخاطر أو وضع الابواب المغلقة بالرموز أو الأبواب الدوارة (Delbecque & Fayol. 2012, p95)
- تركيب أجهزة إنذار في حال التدخل غير المسموح أو في المناطق الحساسة.
- الإضاءة الأتوماتيكية، والمراقبة المستمرة للبناية عن طريق الحراس طول السنة.(Menthonnex , 1995 , p339)
- إغلاق حظيرة السيارات التي توصل إلى البنايات كل مساء وأيضا في الإجازات.
- مراقبة الدخول المادي ووضع كاميرات مراقبة.
- استخدام أجهزة كشف الدخان والإطفاء الآلي للوقاية من الحريق ومكافحته .

ب. أمن تجهيزات نظم المعلومات

ب.1. الحماية المادية لقاعات وأجهزة المعلوماتية: مراقبة الدخول للأنظمة :الوصول المادي للتجهيزات يجب أن تكون ضمن سياسة مراقبة المداخل ومعرفة حاجات ومستويات السرية المسموح بها لكل مستخدم. (Carpentier, 2009 , P39) وإغلاق قاعات الخوادم والمعلوماتية والمكاتب وكل الاجهزة المتحركة التي تضم معلومات مهمة يمكن انتشالها. .(Atelin, 2009 , p 320)

- حماية الكابلات الكهربائية وكابلات التواصل.
- التهوية :يجب أن يكون هناك آلية تهوية موضوعة في خدمة أجهزة أنظمة المعلومات.
- وضع إجراءات لحماية الحواسب المحمولة عند السفر وعند حضور المؤتمرات والندوات كتجنب ترك الأجهزة في الحقيبة الخلفية للسيارة لأن ذلك يعرضها للعوامل الحيوية كالحرارة المرتفعة التي قد تتلف الدوائر الالكترونية في الحاسوب، أو البرودة الشديدة التي تؤدي إلى عطب الشاشة أو يتعرض للسرقة.
- الحماية ضد السرقة بوضع سلك الأمان الذي يربط في موضع خاص بالحاسوب المحمول ويثبت الكابل بهذا الموقع، كما يثبت طرفه الآخر بجسم ثقيل أو ثابت.
- تركيب أنظمة اكتشاف للحماية ضد الحريق والفيضان وتسرب المياه.
- حماية التحاميل، أقراص التخزين، آلات الطباعة والنسخ عن طريق وضع إجراءات مراقبة كل مستعمل لها إلى غاية إرجاعها.

ب.2. الحماية الفنية لأجهزة نظم المعلومات:

– كلمات المرور: الدخول إلى أجهزة العمل والوسائل المتحركة يجب أن تؤمن عن طريق كلمات المرور التي تتضمن معلومات سرية ويجب أن تكون صعبة .

– تغيير كلمة السر كل 6 أشهر أو سنة بالأكثر واستخدام 10 أحرف متنوعة من أحرف كبيرة وصغيرة وأرقام ورموز صعبة لتصعيب اكتشافها.

– تركيب مراقب سري على شاشات الحواسب المحمولة، اللوائح، الهواتف ذات الاستعمال المهني، وفي حال استعمال الويفي والبلوتوث في الأجهزة كثيرة التنقل يجب التذكر ان أي ارتباط يمكن أن يعرضها للخطر.

– تحميل برنامج خفي يسهل متابعة الجهاز في حال السرقة.

ت. انتباه العنصر البشري لتحركاته وتصرفاته (حماية المعلومات الحساسة): العامل الأساسي في تسيير أمن المعلومات الاستراتيجية يتموقع بين الكرسي ولوحة المفاتيح ،ليس الآلة ،إنما العامل البشري، فمن المهم جدا أن ينتبه كل شخص في المؤسسة للتصرفات اليومية البسيطة واعتماد العادات الجيدة لحماية المعلومات الحساسة. (Arnaud & Cuenot ,2003 , pp 41-42)

ت.1. تدابير الحماية داخل المؤسسة:

– **التدابير اليومية:** ومن بين التدابير اليومية ما يلي :

– حماية التوثيق الداخلي للمؤسسة: يجب ترتيب وأرشفة الوثائق بطريقة جيدة وتعريف الوثائق الخاصة بالمؤسسة عن طريق تعليمها.

– عدم ترك المعلومات الناتجة عن الاجتماع مهما كان ما سجلت عليه(ورق ،تحميل).

– النسخ والتخزين الاحتياطي في موقع مختلف كتأمينهم مثلا في مؤسسة خارجية متخصصة في أرشفة الاعلام الآلي.

و من شروط التخزين ما يلي :

– تجديد المعطيات الواجب تخزينها، ومدة التخزين، ومراجعة دورية لمحيط الخزن.

– تعديد أماكن الحفظ والتخزين في عدة تحاميل.

– تأمين أماكن التخزين والحفظ الشهري والسنوي للتحاميل خارج المؤسسة.

– **التدابير الخاصة:** ومن بين التدابير الخاصة ما يلي :

– **التدابير المتخذة مع المتدربين (المستخدمين المؤقتين)**

– التحقق الجيد لمسار المستخدم المؤقت المستقبلي قبل أن يأتي، ودراسة السيرة الذاتية جيدا والاتصال بالجهات المعنية للتأكد من صحة المعلومات المدونة فيها.

– تحسيس المستخدم المؤقت منذ وصوله بمعايير الامن المطلوبة في المؤسسة

– تعيين مسؤول مكلف بتأطير المتدرب ومرافقته ومراقبته.

– وضع بند السرية في العقد، والتأكد من التزامه به .

- **التدابير المتخذة مع الزوار:**
- التحديد المسبق لمسار الزيارة، والابتعاد عن المناطق الخاصة والسرية.
- تدوين المعلومات الخاصة بالزوار واجبارهم على حمل البطاقات الخاصة.
- المرافقة الدائمة للزائر خلال كل الزيارة في حدود المعايير المطلوبة.
- اخفاء الوثائق المهمة عند الزيارات فقد يقوم الزائر بالتصوير بطريقة غير شرعية.
- تحضير حاسب مسبقا غير متصل بالشبكة يسمح باستقبال مفاتيح وتحاميل الزوار.
- استقبال الزيارات بقاعة الاجتماعات،ليس في المكتب أين توجد المعلومات الحساسة.
- **ت.2. تدابير الحماية خارج المؤسسة:** تتضمن الحماية خارج المؤسسة:
- **التحركات المهنية:** من التدابير المتخذة في سفرات العمل ما يلي :
- تحديد إطار محدد لمهمة العمل، وأخذ فقط المعلومات والأجهزة الضرورية وعدم استخدام الأجهزة المتاحة في أماكن العمل.
- التحفظ وتجنب المحادثات المهنية وعدم الوثوق بأي صداقات جديدة.
- **الأماكن العامة:**
- تفادي التكلم في مواضيع العمل في الأماكن العامة فقد تتعرض لخطر التصنت من منافس يجلس بقربك وتفادي قراءة الملفات المهنية بصوت مرتفع أو فتح شاشات الحاسوب في مكان عام، مما قد يعرضك لاستراق النظر من شخص ما.
- عدم التكلم مع شخص مجهول عن أمر متعلق بالعمل، فقد يكون يعمل لدى المنافس.
- تفادي استعمال الويفي والبلوتوث خلال التنقل لتفادي أي ارتباط.

3.3 . الحماية القانونية للممتلكات غير المادية (حقوق الملكية الفكرية)

أ. حماية المصنفات المعلوماتية

أ.1 حماية برامج الحاسوب : تعد برامج الحاسوب أهم مصنفات المعلوماتية أو تقنية المعلومات التي حظيت باهتمام كبير من حيث وجوب الاعتراف وتوفير الحماية القانونية لها، ومن أجل توفير حماية مناسبة للبرنامج يجب أولا إعطاء تعريف محدد له:

-البرنامج هو مجموع الأنظمة ،الإجراءات، القواعد، والتوثيقات المتعلقة بمعالجة المعلومات(Bitan,2010 , p21)

- ويعرف أيضا على أنه: مجموع الأوامر المرتبة التي تتيح للأجهزة المادية للكمبيوتر القيام بمهامها. وبدون البرمجيات تصبح الأجهزة مجرد كتل بدون فائدة.

والبرامج المحمية يمكن أن تكون برامج تشغيلية (Windows) ،أو برامج تطبيقية(Word،Exel)، ويمكن أن يكون برنامج عام أو تحت الطلب.

– وقد أثارت برامج الحاسوب جدلا واسعا بشأن طبيعتها وموضع حمايتها من بين تشريعات الملكية الفكرية، وترددت الآراء بين داع لحمايتها عبر نظم براءات الاختراع لما تنطوي عليه من سمة الاستغلال الصناعي، وبين من ذهب إلى حمايتها عبر نظم الأسرار التجارية إذ تنطوي في الغالب على سر تجاري يتجلى بالأفكار التي انبنى عليها أو الغرض من ابتكارها، وبين داع لحمايتها عبر آلية الشروط العقدية التي تجد مكانها في رخص الاستخدام أو اتفاقيات الاستغلال، لكن كافة هذه الآراء لم تصمد أمام الرأي الذي وجد في البرمجيات عملا ابتكاريا أدبيا، يضعها ضمن نطاق مصنفات الملكية الأدبية، إذ هي أفكار وترتيب لخوارزميات تفرغ ضمن شكل ابتكاري ابداعي، وصفاتها المميزة تتقابل مع عناصر الحماية لمصنفات الملكية الادبية،(يونس عرب، ص 20 www.arablawinfo.com) وبما أن البرنامج هو عبارة عن نتاج العقل، فمن شروط حمايته هو اكتساء طابع " الأصلية " الذي يكون تقييمه غالبا عرضة للجدال، فعنصر الاصلية يعكس ويترجم تعبيرات شخصية المؤلف وبصمته، وهذا يختلف حسب البرنامج. (Bitan,2010 , p30)

و من الاجتماعات والاتفاقيات التي ترسّم حماية البرامج كمصنفات أدبية هي سلسلة اجتماعات خبراء الويبو ومنظمة اليونسكو عام 83 و85 التي أسفرت عن توجه عام لاعتبارها من قبيل الاعمال الادبية، كما أن اتفاقية **تربس** أضافتها إلى المصنفات الأدبية والفنية محل الحماية بموجب اتفاقية بيرن. (يونس عرب، ص 20 www.arablawinfo.com) وتكتسب الحماية منذ ابتكار البرنامج دون أي اجراءات، الشرط الوحيد هو" الأصلية "، كما أن ايداع ملكية حقوق المؤلف ليس اجباري بل محبذ من أجل اقامة الحجة على تاريخ وابتكار البرنامج، وتكون مدة الحماية 70 سنة منذ نشره وتعطي لصاحب البرنامج حق حصري في :إعادة الانتاج، الترجمة، التكييف والترتيب والتوزيع، ومنع إعادة انتاج البرامج جد صارم ،إذ أنه من الممنوع إعادة انتاج جزء أو كل البرنامج سواء بصفة مؤقتة أو دائمة ،و تحت أي شكل وإن كان لأغراض شخصية أو بيداغوجية، وصاحب الحق على البرنامج حر في منح تراخيص استعمال البرنامج مجانية أو مدفوعة (Célarier , 2002 , pp 31-32)

استثنائيا، البرنامج يمكن أن يكون محمي بحقوق البراءات :

– إذا كان الاختراع المحصل على البراءة يضم برنامج، إذن البرنامج بصفة غير مباشرة يصبح محمي ببراءة اختراع.

– إذا كان البرنامج ينتج عنه نتائج تقنية ملموسة، بمعنى يسمح بتحقيق منتج أو أسلوب، وإذا كانت خصائص التسجيل مكتملة إذن يستطيع أن يحصل على براءة الاختراع .

أ.2 حماية قواعد البيانات : البيانات المخزنة في نظم الحواسيب ليست محل حماية بالنسبة للقوانين والأنظمة، لكنها متى ما أفرغت ضمن قاعدة بيانات وفق تصنيف معين وبآلية استرجاع معينة فانها تتحول من مجرد بيانات إلى قاعدة معطيات.

وتعرف قاعدة البيانات على أنها: كتب تحوي مقتطفات أدبية أو وثائق، معطيات أو عناصر أخرى مستقلة، منظمة بطريقة منهجية أو نظامية وسهلة المنال بوسائل الكترونية أو بأي وسيلة أخرى. والاعتراف لقواعد البيانات بالحماية

جاء وليد جهد واسع لمنظمة الويبو ولمجلس أوروبا الذي وضع عام 1996 قواعد ارشادية وقرار يقضي بالنص على حماية قواعد البيانات ضمن قوانين حق المؤلف، كما أن اتفاقية تربس نصت صراحة في المادة 2/10 على تمتع البيانات المجمعة سواء كانت بشكل مقروء آليا أو أي شكل آخر بالحماية القانونية متى ما كانت تشكل خلقا فكريا. (يونس عرب، ص 21(www.arablawinfo.com)

وحقوق منتج قواعد المعطيات أو حقوق Sui generis (حقوق موضوعة خصوصا لحماية قواعد البيانات) تحمي قاعدة البيانات منذ ابتكارها لمدة 15 سنة تُحسب منذ اتمام قاعدة البيانات أو منذ أول وضعها وإتاحتها للجميع.(Célarier , Delphine ,2002 , p 34)

أ.3. حماية موقع الانترنت: الحماية الفكرية المتعلقة بمواقع الانترنت متعددة، حسب محتوى الموقع والأدوات المرافقة له، فإذا كان المحتوى نتاج عقلي يمكن أن يُحمى بعنوان حقوق المؤلف، وإذا كان الموقع يحوي قاعدة معطيات يُحمى عن طريق حقوق Sui generis التي تحمي قواعد البيانات، اسم المجال يمكن أن يحمى عن طريق حقوق العلامة.

حقوق المؤلف تحمي موقع الويب منذ ابتكارها إذا كان أصلي، فالموقع يعكس شخصية المؤلف وتكون مدة الحماية 70 سنة منذ إعلانها إذا كان الموقع نتاج أدبي أو فني جماعي محقق من طرف عدة مؤلفين أين تكون المساهمة الشخصية غير بارزة، أما بالنسبة لموقع ويب مؤلف واحد أو مؤلفين أين تكون مساهمته منفصلة بموضوع ما، الحماية عن طريق حقوق المؤلف تذهب إلى غاية 70 سنة بعد موت المؤلف.

الخاتمة:

أمن نظم المعلومات عبارة عن منظومة متكاملة متكونة من عناصر مادية والمتمثلة في المواقع والأجهزة الضرورية لاحتواء المعلومات والأنظمة المعلوماتية، وعناصر لامادية المتمثلة في العناصر التقنية كالبرامج والتطبيقات الضرورية لعمل أنظمة المعلومات وأهم عنصر وهو العنصر البشري الذي يمثل في نفس الوقت تهديدا وثغرة، ولا يتم تحقيق الأمن إلا من خلال السيطرة على جميع هذه المكونات والتحكم الجيد في جميع التهديدات الممكنة من خلال تطبيق الحماية الملائمة لكل عنصر، ومن جملة الاستنتاجات التي تم التوصل اليها ما يلي :

- التهديدات التي تطال أنظمة المعلومات أصبحت في تطور مستمر، وأصبح من الصعب السيطرة عليها من خلال طرق الحماية التقليدية.
- التهديدات الأكثر خطورة تأتي من الداخل وهي تغطي النسبة الأكبر من التهديدات .
- أمن المعلومات اليوم ضرورة حتمية من أجل بقاء المؤسسة ولم يعد مجرد رفاهية.
- حماية أنظمة المعلومات والمعلومات الحساسة في المؤسسة يجب أن يكون ضمن منظومة متكاملة تضم حماية المكونات المادية والبرمجية واليقظة في التعامل مع العنصر البشري.

المراجع المستعملة

- حسين، أسامة سمير (2011). الطبعة1 .**الاحتيال الالكتروني – الأسباب والحلول** .الجنادرية للنشر والتوزيع.

- عبد الله، الشدي طارق (2000)، **آلية البناء الأمني لنظم المعلومات**، دار الوطن للطباعة والنشر والإعلام، الرياض .

- بن ضبيان. الرشيدي علي.(2000). **العدوان على البيئة المعلوماتية** :خطورته ومواجهته ،مجلة كلية الملك خالد العسكرية، العدد 81، الرياض .

- بيهان. عبد الله بن شائع (2007). **ثقافة أمن المعلومات**. الملتقى الدولي الثالث لأمن المعلومات والاتصالات. سوريا

- الغثير. خالد بن سليمان (2009) مهندس محمد بن عبد الله القحطاني. **أمن المعلومات بلغة ميسرة**. الطبعة الأولى. مكتبة الملك فهد الوطنية. الرياض.

- عرب. يونس، **نظام الملكية الفكرية لمصنفات المعلوماتية**، الدليل الالكتروني للقانون العربي، ArabLawInfo، أنظر: www.arablawinfo.com

- معجم الحاسبات، الطبعة الموسعة، مجمع اللغة العربية، مصر، 1995

- Vaucamps. A., (2010) .CISCO: Sécurité des routeurs et contrôles du trafic réseau, éditions ENI. France.

- Arnaud. P & Cuenot. P., (2003), Intelligence Economique ,mode d'emploi – Maitrisez l'information stratégique de votre entreprise , édition Pearson , France .

- Godart. D., (2005) .sécurité informatique: risques ,stratégies et solution 2éme édition ,éditions des CCI de wallonie s.a Belgique.

- Léopold. E, & Lhoste. S., (2007). la sécurité informatique. 3éme édition. éditions Puf.

- Delbecque. E., & Fayol. J. R., (2012) Intelligence économique , ED Vuibert , paris.

- Bitan. H, (2010). Droit des créations immatérielles –logiciels , bases de données , autres œuvres sur le web 2.0 , éditions Lamy , France .

- Carpentier. J.F, (2009). la sécurité informatique dans la petite entreprise ,ED ENI, France.

- Royer. J.M. (2004). Sécurisé l'informatique de l'entreprise: enjeux , menaces , prévention et parade , édition ENI.

- Menthonnex. M. (1995). Sécurité et Qualité informatiques-Nouvelles Orientation, CERSSI , Presses Polytechniques et Universitaires Romandes , Suisse .

- Laudon. K & Laudon. J. (2006) Management des systèmes d'information. 9éme édition .édition Pearson, ,France.

- Célarier. M. F. (2002). Delphine Marie-Vivien , les droits de propriété intellectuelle :guide pratique , éditions Cirad ,France .

- Lafitte. M, (2003). Sécurité des systèmes d'information et maitrise des risques, édition Revue Banque.

- Atelin. P. (2009). Réseaux informatiques-notions fondamentales- , 3éme édition , édition ENI , France .

- Gallagher. T., Jeffries. & B, Landauer. L., (2007). Chasser les failles de sécurité , les meilleures pratiques pour tester la sécurité de vos logiciels , édition microsoft .

- Whitman. M. & Mattod. H. (2011). Principles of Information Security , 4th Edition, Boston: cengage learning/course technology .

- Menaces sur les systémes informatique « Guide N 65 »(2006). bureau conseil de la direction centrale de la sécurité des systèmes d'information, paris.

الهوامش:

[2]« un virus est programme capable d'infecter d'autres programmes en les modifiant de manière à ce qu'ils contiennent une copie de lui-même, parfois évoluée »

[3] بروتوكول (TCP/IP): هو اللغة الأكثر استخداما في الانترنت للتخاطب وتبادل المعلومات

*بروتوكول (IP) (Internet Protocol): هو نوع من بروتوكولات التواصل للشبكة المعلوماتية، يقدم خدمة تحويل المعطيات تسمى datagrammes من العنوان المصدر نحو عنوان المستقبل، وهذا البروتوكول لا يقدم ضمان للاستقبال الجيد ولا مراقبة المرور، هذا من اختصاص بروتوكولات أخرى مثل .TCP

**بروتوكول TCP (Transmission Control Protocl): مهمته عرض خدمة جد موثوقة في ارسال المعطيات نقطة بنقطة على مستوى شبكة معلوماتية، وهو قادر على تحويل معطيات القاعدة وتحديد وتصحيح أخطاء الارسال ومراقبة المرور، وهو يعمل تحت بروتوكول IP عن طريق اتصال بين عمليتين على حاسبين متباعدين