واقع أمن المعلومات في المؤسسة الوطنية للأشغال البترولية الكبرى

The reality of information security in the National Corporation for Major Petroleum Works " GTP"

تاريخ الاستلام: 2018/08/21 تاريخ قبول النشر: 2019/02/08

فيلالي أسماء د. يحياوي سليمان
طالبة دكتوراه أستاذ محاضر أ
جامعة أبو بكر بلقايد جامعة الجيلالي اليابس
تلمسان – الجزائر. سيدي بلعباس – الجزائر.

الملخص:

تهدف هذه الدراسة إلى تبيان أهمية تطبيق أمن المعلومات على مستوى المؤسسة و التعرض لأنواع التهديدات التي تتعرض لها أنظمة المعلومات و طرق الحماية التي يمكن أن نواجه بها التهديدات المحتملة أو الواقعة ، مع دراسة واقع أمن المعلومات على مستوى المؤسسة الوطنية للأشغال البترولية الكبرى و الجهود التي تبذلها من أجل تطوير نفسها في هذا المجال .

الكلمات المفتاحية :أمن المعلومات ، التهديدات ، طرق الحماية المعلوماتية ، نظم المعلومات ، المؤسسة الوطنية للأشغال البترولية الكبرى

Abstract :

The purpose of this study is to demonstrate the importance of applying information security in the organization, and mention the types of threats to information systems, and the methods of protection, and examine the reality of information security at the level of the National Petroleum Works Corporation and its efforts to develop Itself in this area

Keywords : Information Security, Threats, Information Protection Methods, Information Systems, National Corporation for Major Petroleum Works

*E-mail : filaliasma@outlook.fr **E-mail : Yahiaoui_s@gmail.com

المقدمة:

أمن معلومات المؤسسة هو تحقيق حماية لكل الممتلكات المادية منها كالأجهزة و البنايات ، و غير المادية كصورة المؤسسة و أنظمتها المعلوماتية و بالأخص المعلومات الإستراتيجية و الحساسة ، و التي تعتبر ثروة حقيقية في ظل اقتصاد المعرفة ، فالتهديدات قد تطال إما توفر المعلومة أو سلامتها أو سريتها و أمنها ، و الحفاظ على سرية المعلومات ليس بالأمر الهين بل هو أمر أصبح يتعب الإدارة العليا للمؤسسات خاصة مع وجود شبكات الانترنت التي أحدثت تغييرات جذرية في كيفية نقل المعلومة .

و عليه فان المؤسسة التي تسعى لتحقيق مستوى معين من الحماية عليها انتهاج منهج واضح في هذا المجال ، و رسم سياسة و استراتيجية خاصة بكيفية تطبيق هذا الأمن على مستواها ، فاليوم لم يعد كافيا شراء أحدث برامج الحماية من أجل حماية الأنظمة و المعلومات ، بل أصبح محتما على المؤسسات أن تنظر لهذا المفهوم كمنهج عمل يومي و دائم ، يحمل في طياته عدة أوجه ، و المؤسسات الجزائرية كغيرها من المؤسسات بدأت تفكر في تأمين ممتلكاتها و لكن بطريقة لا تزال محتشمة ، فالمؤسسات التي اهتمت بمجال أمن المعلومات في الجزائر تعد على الأصابع ، من بينها المؤسسة الوطنية للأشغال البترولية الكبرى هذا ما دفعنا إلى طرح الاشكالية التالية:

ما هو واقع أمن المعلومات في المؤسسة الوطنية للأشغال البترولية الكبرى ؟ و ما هي المجهودات التي تبذلها في هذا المجال؟

للاجابة على هذه الاشكالية تم الاعتماد على فرضيتين :

- أمن المعلومات ضرورة حتمية لبقاء المؤسسة و تطورها.
- أمن المعلومات على مستوى المؤسسة الوطنية للأشغال البترولية الكبرى متدني.

هيكل الدراسة :

المحور الأول : ماهية أمن المعلومات

- تعريف امن المعلومات
- تهديدات أمن المعلومات
- طرق تحقيق أمن المعلومات

المحور الثاني : واقع أمن المعلومات في المؤسسة الوطنية للأشغال البترولية الكبرى

-واقع أمن المعلومات في الجزائر

- واقع أمن المعلومات في المؤسسة الوطنية للأشغال البترولية الكبرى
- تحليل نتائج الدراسة

المحور الأول : ماهية أمن المعلومات

1- تعريف أمن المعلومات و عناصره :

1.1 - تعريف أمن المعلومات

يقصد بأمن المعلومات " كل السياسات و الإجراءات و الأدوات التقنية التي تستخدم لحماية النظام من كل أشكال الاستخدام غير الشرعي للموارد مثل : السرقة ، التغيير و التعديل ، إلحاق الضرر بالمعلومات أو قواعد البيانات ، أو إلحاق الضرر المادي المتعمد بالأجهزة ، بالإضافة إلى وجود تهديدات أخرى مثل الاخطاء الإنسانية و الحوادث الطبيعية و الكوارث ".[1]

و عرف Whitman et Mattod أمن المعلومات في كتابهما " مبادئ أمن المعلومات " بأنه " الحفاظ على سرية و توفر و سلامة المعلومات كأصل في مراحل المعالجة و الحفظ و النقل ، و يتحقق ذلك عبر التطبيق الفعلي للسياسات الأمنية و من خلال تعزيز الوعي و التعلم و التدريب.[2] و يرى كلاهما أن أي مؤسسة تهدف لتحقيق ادارة أمن نظم المعلومات فإنه يجب أن يشمل المكونات التالية :

- **الأمن المادي** : بما يشمله من مصادر و ممتلكات و مباني لمنع الوصول غير المشروع.
- **أمن الأفراد** : لحماية الافراد و المجموعات الذين لهم حق الوصول للمعلومات.
- **أمن العمليات** : لحماية الأنشطة و العمليات التي يقوم بها المخولون.
- **أمن الاتصالات** : لحماية الوسائط و التكنولوجيا المستخدمة و المحتوى.
- **أمن الشبكات** : لحماية مكونات الشبكة و التراسل و المحتويات.
- **أمن البيانات** : لحماية سرية و سلامة و توافر المعلومات.

و 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 ، و أمن الأفراد الذين يملكون المعلومات ، و كل العناصر الاخرى التي لها علاقة بالمعلومات.

2.1. عناصر أمن المعلومات

إن المنظمات التي تسعى لتحقيق أمن نظم المعلومات إنما غايتها تحقيق الثالوث المسمى (CIA triangle) و يعني السرية (Confidentiality) ، التكاملية و السلامة (Integrity) ،و التوفر و الإتاحة (Availability).[3]

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 و خصوصية البيانات المخزنة فيه ، فلا يسمح بكشفها بدون ترخيص.

ب- **التكاملية و السلامة (Integrity)** هي بصفة عامة ضمان سلامة محتوى المعلومات ، و التأكد أن هذه المعلومات لم تتعرض لأي عملية حذف أو تخريب أو اتلاف كلي أو جزئي سواء بصفة متعمدة أو غير متعمدة في أي مرحلة من مراحل المعالجة او التبادل و إلا يكون قد تم ضياع تكامل المعلومات.

ج- **التوفر و الإتاحة (Availability) :**و نعني به تمكين المستخدم (إنسان أو نظام حاسوب) الذي له حق التعامل مع المعلومات من ذلك بدون التدخل أو الإعاقة في أداء تلك المهمة ، و وصول المعلومات في الشكل المطلوب.

2- تهديدات أمن المعلومات

يعرف التهديد بصفة عامة على أنه : " هدف عدائي يحمل تحت تصرفه وسائل حقيقية من أجل تعريض مؤسسة ، أشخاص ، مواقع للخطر "[4].

1.2 **مصادر التهديدات** : مصادر تهديدات نظم المعلومات متعددة ، فنجد مثلا المصادر الطبيعية : كالحرائق و الفيضانات و الزلازل و انقطاع التيار الكهربائي ....و نجد المصادر البشرية و هي ما يهمنا خلال البحث ، و هي بدورها تنقسم إلى قسمين :

أ-تهديدات بشرية داخلية : هي التهديدات الصادرة من داخل المؤسسة و التي يتسبب فيها العامل أو الموظف الذي يتعامل مع أنظمة المعلومات ، و له حق الوصول إلى شبكة المنظمة أو أماكن تواجد الأجهزة و المعدات ، أو أي شخص يكون دخوله طبيعيا إلى المؤسسة أو ينتمي إليها، و يكون له نية إلحاق الضرر بأنظمة معلومات المؤسسة أو معلوماتها الحساسة من أجل استخدامها في تحقيق مصالح معينة.

ب- تهديدات بشرية خارجية : هي تهديدات تنفذها هيئات من خارج المنظمة و تكون إما من خلال الانترنت أو خطوط الهاتف نظرا لعدم امتلاكها حق الوصول إلى الشبكة الداخلية للمؤسسة ، و تكمن خطورة هذا النوع من التهديد في عدم أو صعوبة معرفة المخترق و أهدافه من وراء الاختراق ، و مدى الاختراق الذي مس النظام.[5]

و حتى نهاية القرن العشرين مصدر الجرائم المعلوماتية الأكثر خطورة كانت ذات مصدر داخلي صادرة من العمال نظرا لامتلاكهم المعارف ، و قدرتهم في الوصول إلى الأنظمة [6]و مقارنة بين حجم الخطر الداخلي و بين حجم الخطر الخارجي سنذكر بعض الاحصائيات :

وفقا لوكالة FBI تشكل التهديدات الداخلية من 60% إلى 80% من التهديدات التي يتم الإخبار عنها[7].

و حسب دراسة قامت بها Gartner Group على المخطط الأروبي سنة 1997 ، ذكرت المنظمات فيها أن مشكل الأمن هو بنسبة 47% من الأعوان الداخليين (المستخدمين) و يعتبر العمال القدماء مسؤولين بنسبة 10% من الحوادث ، أما الخارجيين فهم مسؤولين بنسبة 39%.[8]

و حسب دراسة أجريت سنة 2003 على 408 خبير معلوماتي يقولون أن 94% من الأدوات المعلوماتية المسؤولة تعرضت لمشكل أمني من مصدر داخلي قام به المستخدمون.[9]

كما كشفت دراسة أجرتها الأمم المتحدة عام 2005 أن 37% من جرائم الاختراق و التعدي داخلي ، و أن 23% يرجع إلى مصادر خارجية ، و بلغ 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 و لم يكتشف سوى 4% منها.[10]

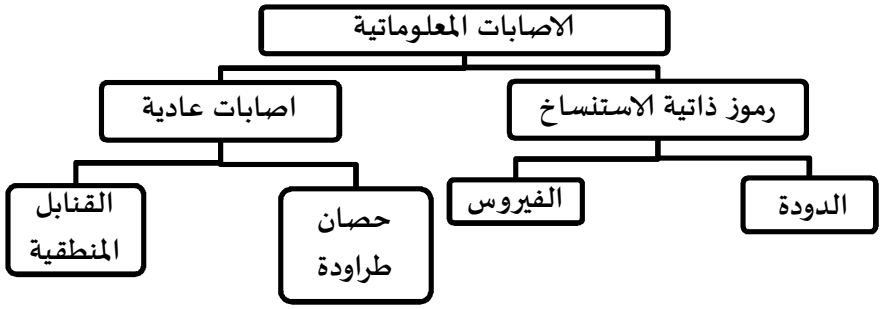
و بخصوص تحصين أنظمة المعلومات فتكون الجهود المبذولة و المسخرة في التحصين ضد التهديد الخارجي على حساب الاستعداد ضد التهديد الداخلي ، في حين هذا الأخير غالبا ما يحدث دمارا باهظ التكاليف ، فحسب تقديرات معهد أمن الحاسوب فإن معدل تكاليف الهجوم الداخلي هو 2.7 مليون دولار للهجوم الواحد ، بينما لا يزيد معدل الهجوم الخارجي الواحد عن 57 ألف دولار.[11]

هذه الدراسات و الإحصائيات أثبتت و بالإجماع أن التهديد الأكبر الذي تتعرض له المؤسسة و أنظمتها المعلوماتية هو من الداخل و بنسب كبيرة جدا مقارنة بالتهديد الخارجي

2.2 أنواع التهديدات : هناك عدة أنواع من التهديدات سنلخصها كالتالي :

أ- الاصابات المعلوماتية : و المتمثلة في البرامج الضارة التي تتعرض لها أنظمة المعلومات ، و أهمها : الفيروس ، الدودة الالكترونية ، حصان طراودة ، القنابل المنطقية.

الشكل 1 : ترتيب الاصابات المعلوماتية



Source : Eric Filiol , les virus informatiques : théorie, pratique et applications , deuxième éditions , Springer , Paris , 2009, p11

ب- القرصنة المعلوماتية (التجسس) : هذا النوع من تقنيات الاعتداء يتمثل في محاولة اقتحام أنظمة المعلومات و الحصول على المعلومات السرية بأي طريقة و من أكثر الطرق انتشارا :

- **التصنت** : التصنت يكمن في التموقع على شبكة معلوماتية أو شبكة التواصل عن بعد ، و من ثم تحليل و تخزين المعلومات العابرة ، و ترجمة التآمرات و كل ما يدور داخل الشبكة المعلوماتية.[12]

- **سرقة الهوية** : سرقة الهوية أو التنكر هو من أنواع السبل غير الشرعية ، تتعلق بهجمة معلوماتية تكمن في انتحال شخصية أو هوية شخص آخر و الاستفادة من امتيازاته و حقوقه عن طريق اغتصاب هويته.

- **رفض الخدمة** : هجمة رفض الخدمة هي تلك التي تعرقل و تمنع خدمة تطبيق ما و جعلها أحيانا غير مفيدة للمستعملين الشرعيين ، باختصار هجمة رفض الخدمة تعمل على ازعاج الضحية ، و لكن أيضا يمكن أن تتسبب في خسائر كبرى.[13]

ج- التهديدات المادية : من بين أهم التهديدات المادية :

ت- السرقة : خصوصا الحواسب المحمولة و التحاميل.

ث- تدمير و تخريب الاجهزة

ج- الهندسة الاجتماعية: هي شكل من أشكال الاستحواذ غير الشرعي للمعلومات و الاحتيال الذي يستغل الثغرات البشرية و الاجتماعية للبنية المستهدفة من أجل الحصول على ممتلك ، خدمة أو معلومات.[14] و قد صنفتها GARTNER سنة 2011 كأكبر خطر في العالم الرقمي للعقد المقبل.[15]

د- **التهديدات الناتجة عن ثغرات أمنية :** الثغرات الأمنية عديدة و متعددة ، و لكي يتم تعدادها بصفة شاملة ، و حسب عدة معايير و مدارس مثل : BS7799 , EBIOS, GMITS من الممكن تجميعها في ثلاث عائلات كالتالي : الثغرات الأمنية على المستوى التنظيمي (الادارة) كضعف التسيير و نقص الكفاءات في هذا المجال و غياب السياسة الأمنية.... ، الثغرات الأمنية على المستوى المادي كنقص التجهيزات و الأعطال... ، الثغرات الأمنية على المستوى التكنولوجي كأخطاء البرمجة و سوء استخدام عناصر المعلوماتية[16].

3- طرق تحقيق أمن المعلومات : تحقيق الأمن المعلوماتي يتطلب منظومة حماية متكاملة من كل الجوانب التي يمكن أن تمس المعلومة :

1.3**الحماية البرمجية** : و تعتبر الحماية البرمجية أهم و أول خطوة في تحقيق الأمن ، و تتمثل في استخدام كل البرامج المتاحة و التي توفر حماية للمعلومات المنتقلة عبر الشبكات أو المخزنة في الحواسيب ، و من أهم البرامج : الجدران النارية ، مضادات الفيروس ، برامج التشفير ، مراقبة الدخول و أنظمة كشف التدخل ، إضافة إلى الشبكة الافتراضية و التحديثات الدورية لهذه البرامج.

2.3الحماية المادية : تحقيق الأمن المعلوماتي لا يكون بحماية المعلومات داخل الحواسب فقط، بل من الضروري تحقيق الأمن الخارجي و المادي للمنظمة و موقع المنظمة و التجهيزات التي تضمها ، فالتهديدات المادية التي تتعرض لها هذه الأخيرة هي الأخطر من بين أنواع التهديدات إذ تدمر كل شيء و لا تترك مجالا للإصلاح ، لذا لا يجب التغافل أبدا عن الحماية المادية لما لها من أهمية لا تقل عن أنواع الحماية الأخرى ، و تكون الحماية بعدة طرق منها : مراقبة الدخول ، اعتماد كاميرات المراقبة ، استخدام الشارات ....

3.3 **الحماية التنظيمية**: أمن المعلومات اليوم لم يعد مرتبطا بتركيب أحدث مضاد للفيروسات أو أقوى جدار ناري أو اعتماد أحدث أدوات المراقبة ، لأن نطاق الأمن توسع جدا و أصبح متعلقا بكل العمليات اليومية داخل المؤسسة ، و لا يمكن التحكم فيه و تحقيق مستوى أمن عالي إلا إذا كان تنظيم هذه العملية واضح للجميع ، فالجانب التنظيمي للأمن هو أهم جانب على مستوى المؤسسة ، إذ أن عملية الأمن عملية دقيقة تتطلب خطة استراتيجية متمثلة أولا في تحضير السياسة الأمنية و وثائقها و تقسيم الأدوار و المسؤوليات و تحسيس و تكوين الموظفين في هذا المجال ، ثانيا من الضروري وضع خطة شاملة لكيفية التعامل مع المخاطر و التي تسمى بعملية تسيير المخاطر و التي من خلالها يتم تحليل بيئة المؤسسة و توقع المخاطر المحتملة و تحليلها باستخدام عدة أدوات و اقتراح معايير المعالجة الضرورية.

4.3 **الحماية القانونية** : و تكون بطريقتين:

- **حقوق الملكية الفكرية** : يوجد اليوم حماية فكرية للمصنفات المعلوماتية تحميها من التقليد و التزوير ، فنجد الحماية المتعلقة ببرامج الحاسوب ، و الحماية الخاصة بقواعد البيانات ، و حماية مواقع الانترنت ، و طوبوغرافيا الدوائر المتكاملة ، و حماية المهارات.
- **القوانين التشريعية** : القوانين التشريعية هي الرادع القوي للقراصنة أو المعتدين بصفة عامة على المعلومات و أنظمة المعلومات ، إذ بتطور المعلوماتية تطورت معها القوانين الخاصة بها ، فسنت قوانين تجرم أفعال التعدي على أنظمة المعلومات ، و تخصيص عقوبات سواء مالية أو السجن تختلف باختلاف حجم الاعتداء و الجهة المستهدفة.

المحور الثاني : واقع أمن المعلومات في المؤسسة الوطنية للأشغال البترولية الكبرى

1- واقع أمن المعلومات في الجزائر

1.1 **من الناحية العملية** : الجزائر بمختلف مؤسساتها من بين الدول التي لا تزال بعيدة نوعا ما عن التطور الأمني الجديد و الذي نجد أثره الجيد فقط في المؤسسات العسكرية ، أما على مستوى المؤسسات الاقتصادية و السلطات المحلية فلا يمكن أن نتحدث عن تعاليم الأمن المعلوماتي ، و هذا بشهادة مجموعة من الدراسات و التحقيقات (تحقيق AASSI ، دراسة Kaspersky lab ، دراسة ألجيريا ديجيتال تراندس) ، و التي أسفرت عن نتائج مقلقة في مجال الاهتمام بأمن المعلومات.

أ- دراسة شركة " ألجيريا ديجيتال تراندس" للتوجيهات الرقمية (2018)

قامت شركة **" ألجيريا ديجيتال تراندس"** للتوجيهات الرقمية بالتعاون مع مؤسسة " رابيد7" الرائد العالمي في قطاع ادارة المخاطر بدراسة احصائية شملت أكثر من 1000 مؤسسة جزائرية و خلصت الدراسة إلى جملة النتائج التالية :

- الشركات الجزائرية لا تزال بعيدة عن المقاييس المفترضة في مجال استخدام التدابير الامنية التي تتضاعف مع التحول الرقمي .

■ أثبتت الدراسة أن 47 % من المؤسسات الجزائرية موضوع الدراسة اعترفت بانعدام أي حماية لنظامها من الهجمات الالكترونية ، و لا تملك أي معرفة بالقوانين المتعلقة بالأمن المعلوماتي ما يجعلها عرضة للقرصنة و الهجمات الالكترونية.

■ 16 % من المؤسسات لا تملك نظم أمن الكتروني و 12 % لا تعرف النظم الأمنية للمعلومات ، و 17 % لازالت تفكر في انشاء نظم حماية.

- 52 % من المؤسسات صرحت أنها لا تملك سياسة لحماية المنظومات المعلوماتية ، و لا موظفين متخصصين و مؤهلين في مجال تقنيات الاعلام و الاتصال .
- 27 % من المؤسسات صرحت أنها عانت مدى 12 شهرا الماضية نوعا من الهجمات المعلوماتية من الفيروسات أو عمليات التصيد الالكتروني ، في حين 12 % عانت فقدان أو تلف البيانات بسبب خطأ بشري.

–57 % من المنظمات تصرح أنها لا تستضيف بياناتها لدى سرفرات جزائرية.

ب– دراسة Kaspersky Lab (2017) :

Kaspersky Lab الرائد العالمي في أمن أنظمة المعلومات أعلن نتائج دراسة وطنية متعلقة بالتصرفات و المواقف المحفوفة بالمخاطر للأمن المعلوماتي للمؤسسات و المنظمات في الجزائر ، هذه الدراسة محققة من قبل مكتب الدراسة و الخبرة CEI حلفاوي ، و هي الاولى من نوعها ، و خلصت الدراسة إلى مجموعة من النتائج :

- 19% " من المهنيين المسؤولين لا يستعملون الحماية المعلوماتية ، ما يظهر مستوى مرتفع نسبيا من الضعف المعلوماتي للمؤسسات و المنظمات الجزائرية.
- 40 % من المجيبين يصرحون أن مؤسساتهم أصيبت بتهديدات معلوماتية : الفيروسات (85 % من المجيبين) ، البرامج الضارة (58 %) ، البرامج التجسسية (29%) و هي أكثر التهديدات تكررا.
- 68 % من المهنيين المسؤولين قد وضعوا تحاميل غير معروفة على حواسبهم و 19 % يفتحون ملفات مرافقة في رسائل مجهولة.
- 72 % من المهنيين يستعملون شبكات التواصل الاجتماعي في العمل و 43 % من المجيبين لا يغيرون كلمات المرور ، ما يفاقم مخاطر التدخل و التجسس.
- 54 % من المجيبين يصرحون بعدم معرفة استخدام أدوات الحماية المعلوماتية ، ما يمثل مستوى ضعيف من التحسيس و التكوين لمختلف طرق الحماية المعلوماتية.
- 56% من المهنيين المستجوبين هم مدركين بالهجمات الالكترونية الحديثة ، ما يدفع 87 % من المجيبين على القول أنهم متيقظين ضد الهجمات الالكترونية.
- 89 % من المهنيين المستجوبين قالوا أنهم مقتنعين أن تواجد هذه التهديدات يتطلب حماية معلوماتية.

ح- تحقيق الجمعية الجزائرية لأمن نظم المعلومات (AASSI) (2015)

تم عمل تحقيق من قبل الجمعية الجزائرية لأمن نظم المعلومات على مجموع المؤسسات و المنشآت الجزائرية حول أنظمة المعلومات و أسفر التحقيق عن النتائج التالية :

- 1 % من المؤسسات و المنشآت يستعمل معيار أمن نظم المعلومات مثل ايزو 27001.
- 7.5 % ليس لديهم اجراءات الامتثال لتكنولوجيا المعلومات .
- 10/1 ليس لديهم مخطط استئناف النشاط.
- 1 % من المؤسسات يصرحون أن لديهم سياسة تسيير الثغرات.

و حسب تصريح مهدي زكريا رئيس الجمعية فان :

- لا يمكن أن نتحدث عن تعاليم أو عقيدة الأمن المعلوماتي عند مقرري تكنولوجيا الاعلام الجزائريين.
- أكثر الهجمات سببها قلة المعرفة التقنية و استغلال الثغرات المعروفة المرتبطة غالبا بسذاجة الضحية مثل هجمات احتيال الشخصية.
- هجمات رفض الخدمة DoS من الصعب اكتشافها في الجزائر ، و لكن ما هو أكيد أن مجموع المختصين في الأمن يقولون أن الجزائر تواجه كل سنة عدة مئات من هجمات رفض الخدمة تشوش على وسائل التواصل للبلد.

2.1 **من الناحية القانونية** : من الناحية القانونية نجد أن المشرع الجزائري بدأ يولي أهمية للقوانين المتعلقة بحماية أنظمة المعلومات و ذلك من خلال بعض القوانين و التعديلات منها تعديل قانون العقوبات بالقانون رقم 04-15 و الذي أفرد فيه قسم 7 مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات " و الذي تضمن 8 مواد (من المادة 394 مكرر إلى المادة 394 مكرر7) ، كما أصدر المشرع الجزائري قانونا مستقلا و هو القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، إضافة إلى الاتفاقيات الدولية التي أبرمتها الجزائر لمكافحة الجريمة المعلوماتية ، و لكن رغم هذه المجهودات إلى أن المشرع الجزائري و الجزائر ككل تبقى متأخرة في مجال حماية و أمن أنظمة المعلومات سواء من الناحية المادية أو البرمجية أو التنظيمية أو القانونية.

2- واقع أمن المعلومات في المؤسسة الوطنية للأشغال البترولية الكبرى

1.2- تعريف المؤسسة :

هي المؤسسة الوطنية للأشغال البترولية الكبرى و التي تعرف ب " GTP " ، مؤسسة ذات أسهم ، فرع تابع 100 % لمجمع سونطراك ، يقدر رأسمالها الاجتماعي ب 6.390.000.000 دج و يقدر رقم أعمالها السنوي حوالي 25 مليار دج سنويا .تمتلك المؤسسة رأسمال بشري مقدر بحوالي 10.000 عامل موزعين كالتالي : 74% منتجين ، 17 % أعوان و 9% إداريين ، أما بالنسبة للتجهيزات فالمؤسسة تمتلك حوالي : 5.600 وحدة من تجهيزات التشييد.

المؤسسة الوطنية للأشغال البترولية الكبرى هي مؤسسة ذات امتداد كبير على المستوى الوطني متخصصة في البناء في جميع الحرف والمجمعات الصناعية الكبيرة ، وخطوط الأنابيب في مجالات النفط والغاز والطاقة بشكل رئيسي.

تقع المؤسسة في مدينة الرغاية بشرق ولاية الجزائر العاصمة ، و يعتبر ذلك المقر الرئيسي لها و تملك 6 وحدات على المستوى الوطني موزعة كالتالي : الرغاية (المقر الاجتماعي) رمزه 01،أرزيو رمزه 02،سكيكدة رمزه 03،حاسي مسعود رمزه 04،حاسي الرمل رمزه 05،عين أميناس رمزه 06.

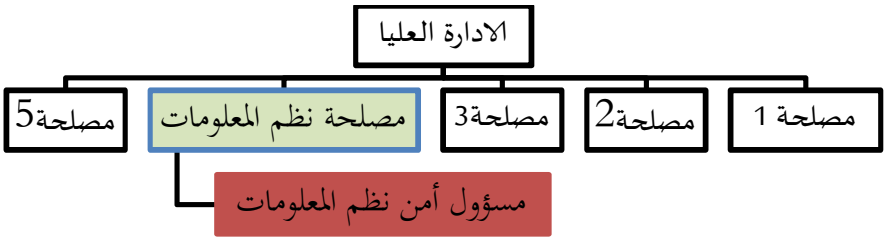
2.2واقع أمن المعلومات في المؤسسة :

أ- مكانة أمن المعلومات على المستوى التنظيمي

- **وظيفة أمن المعلومات على مستوى المنظمة:**

المؤسسة الوطنية للأشغال البترولية الكبرى من بين المؤسسات الجزائرية القلة التي نجدها تخصص وظيفة لأمن نظم المعلومات ، إذ هناك مصلحة خاصة في المنظمة تسمى مصلحة نظم المعلومات ، و تتكون من رئيس المصلحة و مختصين في مجال أنظمة المعلومات و الاعلام الآلي ، و هناك مسؤول أمن نظم المعلومات مسؤول عن أمن حواسب و تجهيزات نظم المعلومات و المعلومات الحساسة و الموارد الحرجة في المصلحة و كل المؤسسة.

الشكل2 : مكانة مسؤول أمن المعلومات في تنظيم المؤسسة



المصدر: من إعداد الطالبة

- **سياسة أمن المعلومات في المؤسسة :**

المؤسسة الوطنية للأشغال البترولية الكبرى تعتمد سياسة أمن معلومات واضحة المعالم و محددة القواعد و المبادئ و يتم نشرها الكترونيا على مستوى موقع المؤسسة ليتم الاطلاع عليها من قبل كافة الموظفين.

- **وعي الادارة و الموظفين :**

رغم اهتمام المؤسسة بأمن نظم المعلومات و تسخير كل الوسائل المادية و البشرية و التقنية لذلك، إلا أن وعي الادارة العليا بخطر التهديدات على نظم المعلومات منخفض ، كما أن الثقافة

الأمنية للموظفين ليست بالمستوى المطلوب ، إذ نجد أن أمن المعلومات يطبق فقط من الناحية المادية التي تتمثل في أمن المحيط ، و من الناحية التقنية من برامج مطبقة على الحواسب و الخوادم ....، أما الوعي الحقيقي و اليقظة الاستراتيجية بخطر التهديدات و أهمية الأمن نجده فقط على مستوى مصلحة نظم المعلومات ، التي تحاول جاهدة تعزيز الثقافة الأمنية على مستوى المؤسسة.

- **المؤسسة و ايزو 27001:**

المؤسسة اهتمت بضرورة تطابق أمن المعلومات لديها بمعايير و مقاييس دولية معترف بها عالميا، و وقع اختيارها على أشهر معيار خاص بأمن نظم المعلومات و هو معيار ايزو 27001 ، حيث باشرت كل الاجراءات اللازمة من أجل الحصول على شهادة ايزو 27001 و كيفت أنظمة معلوماتها و سياستها الأمنية و طرق الحماية حسب متطلبات المواصفة ، و حصلت على شهادة ايزو 27001 سنة 2010 لمدة 3 سنوات ، و لكن للأسف المؤسسة لم تستمر في عملية التجديد ، لأن هذه الشهادة ليست أبدية كباقي الشهادات ، و إنما تكون لفترة معينة و تتطلب في كل مرة التجديد و التحقيق من أجل أن تكون المؤسسة دائما في المستوى المطلوب.

ب- تهديدات أمن المؤسسة

المؤسسة كغيرها من المؤسسات الكبرى تتعرض إلى تهديدات عدة منها المادية مثل السرقة و الكوارث... و منها التقنية كالقرصنة ، و من التهديدات التي تعرضت لها المؤسسة ما يلي :

- **التهديدات المادية :**

- الدخول غير المصرح : و يقصد به دخول أي شخص معروف أو غير معروف ، غير مرخص له بالدخول إلى موقع المنظمة ، فمجرد دخوله يعتبر خطر على المؤسسة.
- سرقة التجهيزات : حيث تعرضت المؤسسة لعمليات سرقة تمت عن طريق اقتحام موقع المؤسسة بطريقة غير شرعية و سرقة تجهيزات خاصة بالمؤسسة.
- كوارث طبيعية : تعرضت المؤسسة لمرة واحدة فقط و ذلك على مستوى فرع من فروعها لكارثة طبيعية كلفتها بعض الخسائر.

- **التهديدات التقنية** : من بين التهديدات التقنية التي تعرضت لها المؤسسة ما يلي :

- دخول غير مرخص : و نقصد هنا الدخول لجهاز أو نظام معلومات من طرف شخص غير مصرح له بذلك ، سواء كان من داخل (العمال) أو من خارج المؤسسة (الهاكر).
- قرصنة : و كانت هذه القرصنة خارجية من طرف هاوي ، و خلفت آثار بسيطة.

- سبام
- الدودة المعلوماتية : فالمؤسسة كغيرها من المؤسسات لم تسلم من خطر هذا البرنامج الخبيث و تم التعامل مع هذه التهديدات باتخاذ عدة إجراءات نذكر منها : إجراءات تصحيحية ، تعديل الاعدادات ، تحقيقات داخلية ، تعزيز أمن محيط المؤسسة ، تغيير كلمات المرور ....

ج- وسائل الحماية المطبقة من طرف المؤسسة

الحماية المطبقة من طرف المؤسسة هي حماية مادية و برمجية

- **حماية مادية** : و تتمثل الحماية المادية في حماية الموقع و حماية التجهيزات من خلال مجموعة من الاجراءات منها :

- مراقبة الدخول : و يكون ذلك من خلال مكتب الاستقبال الموجود في مدخل المنظمة يضم عدد كبير من أعوان الأمن ، و يمنع أي دخول للمؤسسة دون المرور عليه .
- الشارات : إجبار الزوار على حمل شارات تميز بين الزوار و العمال و المتدربين.
- مرافقة عون الأمن للزائر إلى المكان المحدد من أجل منع أي دخول إلى موقع غير مصرح له.
- استخدام البطاقات الممغنطة من أجل الدخول.
- المراقبة عن طريق الكاميرات الموجودة في كل مكان داخل و خارج المؤسسة .
- منع دخول أي سيارة للمؤسسة غير سيارات العمال.
- توفير التهوية المناسبة خصوصا للغرف التي تحوي أجهزة و خوادم ، و التي تتطلب مستوى تهوية محدد.
- التجهيزات الحساسة موجودة في أماكن محددة و مؤمنة بطريقة مكثفة.
- المؤسسة لديها مركز احتياطي مجهز بأنظمة معلومات في حال حصول كارثة يتم اللجوء إليه.

- **حماية برمجية** : و تتمثل في البرامج و التطبيقات التي تحمي أجهزة نظم المعلومات و نذكر :

- مضادات الفيروسات : و هي القاعدة الأولى لأي حماية برمجية ، حيث أن المؤسسة لا تعتمد على البرامج المقرصنة و إنما تشتري برامج مضادات فيروس أصلية.
- مضادات السبام
- الجدران النارية : فالمؤسسة تعتمد على الجدران النارية المتمثلة في أجهزة مخصصة لذلك و ليس تلك التي تكون في شكل برامج.
- التشفير : و نقصد بذلك تشفير كل المعلومات الحساسة المرسلة سواء عند التواصل مع فروعها أو مع أعوان خارجية
- الشبكة الافتراضية و الدعم الاحتياطي

- الحفظ الدوري للمعلومات داخل و خارج المؤسسة و التحديث الدوري لبرامج الحماية.
- تغيير كلمات المرور من فترة لأخرى أو عند حصول أي اختراق.

3- **تحليل نتائج الدراسة** :

1.3- **عينة الدراسة** : تمثل مجتمع الدراسة في المؤسسة الوطنية للأشغال البترولية الكبرى ، و تمثلت عينة الدراسة في موظفي ادارة نظم المعلومات فقط و هم 8 أشخاص ، و هذا نظرا لخصوصية الموضوع و عدم امكانية الاجابة على الاستبيان من غير المتخصص.

2.3 – **أساليب جمع البيانات** : تم الاعتماد في جمع البيانات على الملاحظة و المقابلة الشخصية مع مسؤول أمن نظم المعلومات ، و أهم وسيلة هو الاستبيان الذي تم توزيعه كما ذكرنا سابقا على عمال مصلحة نظم المعلومات ، حيث تم تصميم الاستبيان وفق سلم ليكرت الخماسي.

3.3- **تحليل النتائج** : قبل بدء التحليل لابد من اختبار مدى ثبات أداة القياس و الذي تم عن طريق اختبار معامل " ألفا كرونباخ" ، و الذي تتراوح قيمته بين 0 و1 و انخفاض قيمته عن 0.6 دليل على انخفاض الثبات الداخلي و كانت النتيجة على النحو التالي :

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,812	24

أما بالنسبة لقراءة المتوسط الحسابي فهي كالتالي :

المتوسط	المستوى
من 1 إى 1.79	أبدا
من 1.80 إلى2.59	نادرا
2.60 إلى 3.39	محايد
من 3.40 إلى 4.19	في معظم الأحيان
من 4.20 إلى 5	دائما

أولا : نتائج البعد الأول : طبيعة الأمن دخل المؤسسة

Statistiques descriptives

	N	Moyenne	Ecart type
الادارة العليا واعية بأهمية و ضرورة توفير الأمن لأنظمة المعلومات	8	3,1250	1,45774
اجراءات الحماية التي تطبقها المؤسسة تواكب التغيرات الحاصلة في البيئة التكنولوجية	8	4,0000	1,30931
المصاريف التي تصرف على تطبيق أمن المعلومات ضرورية و تساهم في حماية المؤسسة و تطورها	8	4,5000	,75593
المؤسسة تعتمد سياسة أمنية مكتوبة و يعرفها الجميع	8	4,0000	1,30931
قواعد و مبادئ السياسة الأمنية محددة و واضحة	8	4,1250	,99103
الموظفون ذوي ثقافة أمنية و واعون بمسؤولياتهم	8	2,3750	1,18773
المؤسسة تقوم بدورات تكوينية و تحسيسية حول موضوع أمن المعلومات	8	3,8750	,83452

نتائج برنامج SPSS.19

يبين الجدول أعلاه متوسط الاجابات و الانحراف المعياري لكل سؤال على حده ، و عليه سنقوم بتحليل كل سؤال على حده :

- **الادارة العليا واعية بأهمية و ضرورة توفير الأمن لأنظمة المعلومات :**

كان متوسط الاجابات 3.125 بمعنى أن الادارة العليا واعية نوعا ما بأهمية و ضرورة توفير أمن نظم المعلومات .

- **اجراءات الحماية التي تطبقها المؤسسة تواكب التغيرات الحاصلة في البيئة التكنولوجية**

متوسط الاجابات 4 بمعنى أن اجراءات الحماية التي تطبقها المؤسسة لحماية أنظمة المعومات و المعلومات الحساسة متطورة و تواكب التغيرات و التطورات الحاصلة في البيئة التكنولوجية.

- **المصاريف التي تصرف على تطبيق أمن المعلومات ضرورية و تساهم في حماية المؤسسة و تطورها :**

متوسط الاجابات على هذه العبارة 4.5 يعني أنه دائما تكون المصاريف التي تصرف على أمن المعلومات ضرورية و تساهم في حماية المؤسسة ، بمعنى أن مصاريف الأمن هي استثمار يعود على المؤسسة بأرباح أخرى و ليس مصاريف زائدة ، كما أن الانحراف المعياري لهذه العبارة 0.75 ما يدل على أن نسبة التشتت قليلة.

- **المؤسسة تعتمد سياسة أمنية مكتوبة و يعرفها الجميع و قواعد و مبادئ السياسة الأمنية محددة و واضحة**

متوسط اجابات هاتين العبارتين 4 و 4.12 على التوالي ما يدل على أنه في معظم الأحيان تعتمد المؤسسة في تسيير عملية الأمن لديها على سياسة أمنية مكتوبة يعرفها الجميع و بمبادئ و قواعد أمنية محددة و واضحة للجميع ، و غالبا ما يتم نشر هذه السياسة على موقع المؤسسة ليتمكن الجميع من الاطلاع عليها

- **الموظفون ذوي ثقافة أمنية و واعون بمسؤولياتهم:**

متوسط اجابات هذه العبارة 2.37 أي أنه نادرا ما يمتلك الموظفون ثقافة أمنية ، فالأمن منحصر فقط في الموظفين المختصين بهذا المجال أما الآخرون فهم بعيدين كل البعد عن كل ما يخص أمن الملومات رغم **التوعية و التحسيس و التكوين** التي ظهر أن متوسط اجاباتها 3.87 بمنى أن المؤسسة في معظم الاحيان تقوم بدورات تكوينية و تحسيسية في هذا المجال ، إلا أن ذلك لم يؤثر كثيرا على الثقافة الأمنية للعمال .

ثانيا : نتائج البعد الثاني طبيعة التهديدات

Statistiques descriptives

	N	Moyenne	Ecart type
التهديدات التي تتعرض لها المؤسسة هي من مصادر داخلية	8	3,7500	,88641
التهديدات التي تتعرض لها المؤسسة هي من مصادر خارجية	8	2,5000	,92582
التهديدات التي تتعرض لها المؤسسة عبارة عن برامج خبيثة : فيروس ، دودة ، حصان طراودة.....	8	4,1250	,99103
التهديدات التي تتعرض لها المؤسسة عبارة عن قرصنة معلوماتية : التصنت ، رفض الخدمة ، التزوير	8	1,5000	,53452
التهديدات التي تتعرض لها المؤسسة ناتجة عن سوء التسيير و نقص الكفاءات البشرية في مجال أمن المعلومات	8	4,0000	,53452
التهديدات التي تتعرض لها المؤسسة ناتجة عن ثغرات أمنية في الأنظمة و البرامج	8	2,6250	1,06066

نتائج برنامج SPSS .19

- **التهديدات التي تتعرض لها المؤسسة هي من مصادر داخلية**

متوسط اجابات هذه العبارة 3.75 أي أن مصدر التهديد في معظم الأحيان يكون مصدر داخلي سواء عمال أو متدربين ... ، و هذه الاجابة تتماشى مع الواقع و هذا بتأكيد العديد من الاحصائيات التي تم ذكرها سابقا ، و بانحراف معياري مقبول 0.88

- **التهديدات التي تتعرض لها المؤسسة هي من مصادر خارجية**

متوسط اجابات هذه العبارة 2.5 ما يدل على أنه نادرا ما تتعرض أنظمة معلومات المؤسسة لتهديدات من مصادر خارجية و هذا راجع لطبيعة الحماية القوية التي تطبقها المؤسسة ما يصعب عملية اختراقها من قبل أي غريب ، و كانت الاجابات متقاربة بانحراف معياري 0.92.

- **التهديدات التي تتعرض لها المؤسسة عبارة عن برامج خبيثة : فيروس ، دودة ، حصان طراودة.....**

متوسط الاجابات على هذه العبارة 4.12 بمعنى أن التهديدات التي تطال أنظمة معلومات المؤسسة غالبا ما تكون متمثلة في البرامج الخبيثة.

- **التهديدات التي تتعرض لها المؤسسة عبارة عن قرصنة معلوماتية : التصنت ، رفض الخدمة ، التزوير**

متوسط الاجابات 1.5 بانحراف معياري ضعيف 0.5 ما يدل على أن المؤسسة لا تتعرض أبدا لتهديدات من هذا النوع ، و هذا راجع لفعالية أنظمة الحماية المطبقة من طرف المؤسسة.

- **التهديدات التي تتعرض لها المؤسسة ناتجة عن سوء التسيير و نقص الكفاءات البشرية في مجال أمن المعلومات**

متوسط الاجابات على هذه العبارة 4 ما يدل على أنه في معظم الأحيان التهديدات التي تمس أنظم المعلومات أو المعلومات تكون ناتجة عن نقص كفاءات في مجال الأمن و هذا يتوافق مع اجابات العبارة الأولى (تهديدات داخلية) ، فنقص الكفاءات في مجال الأمن يؤدي إلى ارتفاع التهديدات الداخلية المرتكبة سواء من طرف العمال أو المتدربين أو الزوار ، كما أن الانحراف المعياري لهذه العبارة 0.5 يدل على شبه اتفاق على ذلك.

- **التهديدات التي تتعرض لها المؤسسة ناتجة عن ثغرات أمنية في الأنظمة و البرامج**

متوسط الاجابات على هذه العبارة 2.62 بمعنى أن الاجابات محايدة فيما يخص الثغرات و هذا الامر طبيعي لأن الثغرات الأمنية لا تكون مكشوفة و معروفة للجميع .

ثالثا : نتائج البعد الثالث : طبيعة الحماية المطبقة

Statistiques descriptives

	N	Moyenne	Ecart type
المؤسسة تعتمد على كاميرات المراقبة لحماية الموقع و التجهيزات	8	4,3750	,51755
المؤسسة تعتمد على مراقبة الدخول عن طريق حمل الشارات و مرافقة الزوار لمنع أي تجاوزات	8	4,6250	,51755
المؤسسة تعتمد على أجهزة الانذار عند أي تدخل غير مسموح لحماية موقعها	8	2,5000	1,30931
المؤسسة تعتمد على مضادات الفيروس لحماية أنظمتها المعلوماتية	8	4,8750	,35355
المؤسسة تعتمد على الجدران النارية لحماية أنظمتها المعلوماتية	8	4,5000	,53452
المؤسسة تعتمد على برامج لتشفير كل البيانات و الاتصالات و التطبيقات المتنقلة و المخزنة لحمايتها من التصنت	8	3,8750	1,24642
المؤسسة تعتمد على أنظمة كشف التدخل لحماية أنظمتها المعلوماتية من أي دخول غير مصرح	8	3,3750	,91613
المؤسسة تعمل على تحديث برامج الحماية دوريا	8	3,6250	,74402
المؤسسة تقوم باختبار أنظمة الحماية دوريا لاكتشاف الثغرات	8	3,3750	,91613
تتم معالجة الثغرات المكتشفة فورا	8	2,1250	,99103
فريق الأمن يعتمد طرق النسخ الاحتياطية المخزنة و الرجوع إليها في حالة الكوارث	8	4,2500	,70711
المؤسسة لديها مخططات لاستئناف العمل بعد حدوث أي طارئ	8	3,3750	1,18773

نتائج برنامج SPSS

- **الحماية المادية** : العبارة 14 و15 كان متوسط اجاباتها 4.37 و 4.62 ما يدل على أن المؤسسة دائما ما تعتمد على كاميرات المراقبة ، و مراقبة الدخول و حمل الشارات و مرافقة الزوار في تأمين موقعها و محيطها المادي ما يعني أن الحماية المادية داخل المؤسسة مرتفعة و هذا بانحراف معياري قدر ب 0.5 ، إلا أن العبارة رقم 16 كان متوسطها 2.50 ما يعني أن المؤسسة نادرا ما تعتمد على أجهزة الانذار عند التدخل لحماية موقعها
- **الحماية البرمجية** : العبارات 17-18-19-20-21-22-23 خاصة بالحماية البرمجية التي تطبقها المؤسسة ، فمتوسط اجابات العبارة 17 و 18 هو 4.87 و 4.50 على التوالي ما يدل على أن المؤسسة دائما تعتمد على مضادات الفيروس و الجدران النارية لحماية أنظمتها المعلوماتية أما العبارات 19 و 21 فكان متوسط اجاباتها على التوالي 3.87 و 3.62 بمعنى أن المؤسسة في

معظم الأحيان تعتمد برامج لتشفير كل البيانات و الاتصالات و التطبيقات المتنقلة و المخزنة لحمايتها من التصنت ، إضافة إلى التحديث الدوري لهذه البرامج ، أما العبارات أما العبارات 20 و 22 المتعلقة باستخدام أنظمة كشف التدخل و اختبارات أنظمة الحماسة لاكتشاف الثغرات فكانت متوسطاتها 3.37 و 3.37 أي اجابات حيادية ، و العبارة 23 الخاصة معالجة الثغرات فور اكتشافها فكان متوسط الاجابات 2.12 أي نادرا ما يتم اكتشاف الثغرة فور اكتشافها.

- **فريق الأمن يعتمد طرق النسخ الاحتياطية المخزنة و الرجوع إليها في حالة الكوارث**

متوسط اجابات هذه العبارة 4.25 أي أن المؤسسة دائما تعتمد طرق النسخ الاحتياطية المخزنة و الرجوع إليها في حالة الكوارث بل و تخصيص مركز احتياطي مجهز يتم استخدامه حالة الطوارئ.

- **المؤسسة لديها مخططات لاستئناف العمل بعد حدوث أي طارئ**

متوسط اجابات هذه العبارة هو 3.37 و هي اجابة محايدة ربما لعدم اطلاع جميع موظفي المصلحة على ذلك ، لكن بتأكيد مسؤول أمن المعلومات فالمؤسسة دائما لديها مخططات استئناف تعود اليها حالة الكوارث

الخاتمة:

أمن المعلومات هو من جهة تأمين المؤسسة تأمينا ماديا يمنع أي دخول مادي غير مرخص للمؤسسة خصوصا المناطق الحساسة فيها كالقاعات التي تضم الأجهزة المعلوماتية ، و من جهة أخرى مواكبة العصر في كل ما يتعلق بالحماية الفنية و البرمجية للأجهزة المعلوماتية من برامج حماية و منع الدخول و كلمات مرور...، و لكن أهم و أكبر مجهود يمكن أن تقوم به أي مؤسسة في مجال أمن المعلومات هو تطوير العامل البشري في هذا المجال ، فكل أنواع الحماية المذكورة سابقا لا تجدي نفعا دون رأس مال بشري واع و محسس بشكل كافي ، فالحلقة الأقوى في تطبيق الأمن هو الفرد الذي أثبتت كل الدراسات أنه سبب أغلب الهجمات و التهديدات التي تتعرض لها المؤسسات و الأنظمة ، و لهذا فعلى كل مؤسسة أن تغير نظرتها حول أمن المعلومات من المنظور الضيق المحصور في الماديات إلى المنظور الواسع و الشامل ، و تبادر بإنشاء سياسات أمن معلومات ترسم الطريق لكيفية التطبيق الصحيحة له.

و من أهم **النتائج** التي تم التوصل اليها من خلال هذا البحث :

- أمن المعلومات لا ينحصر في مجموعة من الأنظمة و البرامج بل هو منهج و منظومة متكاملة.
- أمن المعلومات لا يحمي فقط المؤسسة من الأخطار بل يدفع بها إلى التقدم و يجعلها في مصاف المؤسسات العالمية.

- أمن المعلومات أصبح ضرورة حتمية لكل مؤسسة تسعى لاثبات تواجدها على الساحة ، و لم يعد مجرد رفاهية ، و هذا ما سؤكد صحة الفرضية الأولى (**أمن المعلومات ضرورة حتمية لبقاء المؤسسة و تطورها.**)

- الجزائر و المؤسسات الجزائرية بعيدة تماما عن هذا المفهوم الجديد.

- المؤسسات الجزائرية التي تطبق أمن المعلومات بالمعايير المطلوبة عالميا تعد على الأصابع.

- المؤسسة الوطنية للأشغال البترولية الكبرى من المؤسسات التي سلكت طريق تطبيق الأمن حسب المعايير العالمية ، خصوصا بعد اهتمامها بالمواصفة العالمية الخاصة بتطبيق أمن المعلومات الايزو 27001 و تسعى جاهدة لتطوير نفسها في هذا المجال سواء من الجانب المادي أو البرمجي أو التنظيمي و هذا ما ينفي الفرضية الثانية نسبيا (**أمن المعلومات على مستوى المؤسسة الوطنية للأشغال البترولية الكبرى متدني**)

المراجع

[1]. سعد غالب ياسين ، تحليل و تصميم نظم المعلومات ، دار المناهج للنشر ،عمان ،الأردن ، الطبعة الأولى ، 2000 ، ص 349.

[2] Whitman Michael , Mattod Herbert , Principles of Information Security , 4th Edition , Boston: cengage learning/course technology , 2011.

[3] Whitson , G , Computer Security : theory, process and management, the journal of computing in small colleges, vol.18, no.6, 2003, p 57.

[4] Eric Delbecque , Jean-Renaud Fayol , Intelligence économique , ED Vuibert , paris 2012 , p 89.

[5] محمد دباس الحميد ، ماركو ابراهيم نينو ، حماية انظمة المعلومات ، دار الحامد للنشر و التوزيع ، عمان ، الأردن ، 2009 ، ص ص 39-40

[6] Kenneth Laudon et Jane Laudon , Management des systèmes d'information , édition Pearson, 9éme édition , France, 2006, p 355.

[7] See :Cisco systems ,inc :Indiana, cisco press, cisco networking academy, first year companion guide , 2nd ed, 2001, p 20.

[8]Didier Godart, sécurité informatique : risques , stratégies et solutions , 2éme édition , éditions des CCI de wallonie s.a , Belgique ,2005 p23.

[9] Ibid , p23.

[10] الرشيدي علي بن ضبيان ، العدوان على البيئة المعلوماتية : خطورته و مواجهته ، مجلة كلية الملك خالد العسكرية، العدد 81 ، الرياض ، 2005 ، ص 12.

[11] " Internal threat-Risks and countermeasures", 15/12/2001 in : http://www.sans.org/rr/papers/60/475.pdf.

[12] Menaces sur les systèmes informatique « Guide N 65 », bureau conseil de la direction centrale de la sécurité des systèmes d'information , paris , version du 12 septembre 2006 , p13

[13] Tom Gallagher, Bryan Jeffries, Lawrence Landauer, Chasser les failles de sécurité , les meilleures pratiques pour tester la sécurité de vos logiciels , édition microsoft ,Janvier 2007, p375.

[14] Pierre-Luc Réfalo , la sécurité numérique de l'entreprise « l'effet papillon du hacker » , groupe Eyeolles , Paris, p49

[15] Ibid , p 49.

[16] Vulnérabilités , fiche thématique 013 , CASES , Cyberworld Awareness and Security Enhancement Structure , Luxembourg , www.cases.lu