العدد السابع - الجزء الاول - يوليو - 2021 - السنة الثانية مجلة علمية فصلية محكمة

المجلة الأمريكية الدولية للعلوم الإنسانية والاجتماعية

American International Journal of Humanities and Social Sciences

ISSN - 2710 - 4834 / رقم الايداع في دار الكتب والوثائق العراقي : 2460

تصدر عن الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب

ISSUED BY AMERICAN INTERNATIONAL ACADEMY OF HIGHER EDUCATION AND TRAINING

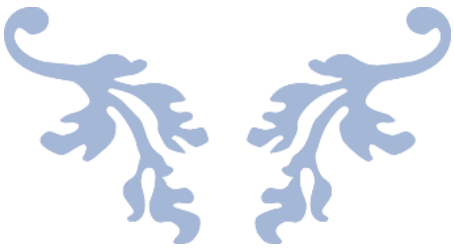
الموقع الرسمي للمجلة / www.aijhssa.us


بسم الله الرحمن الرحيم

أعضاء الهيئة العلمية

أعضاء الهيئة الاستشارية

مقال العدد



بسم الله الرحمن الرحيم ، الحمدّ لله على فضله ونعمته ، والصلاة والسلام على رسوله الكريم وآله ، أمّا بعد ..

يضّم العدد السابع من المجلة بين دفتيه بحوث المؤتمر العلميّ الدوليّ الثالث للأكاديمية الأمريكية للتعليم العالي والتدريب الذي تجلى بشعار " التنمية المستدامة بين القطاعين ؛ الحكومي ، والخاص ، في تحقيق أهدافها " ، وانعقد للمدة من الثاني حتى التاسع من كانون الثاني / يناير لعام ألفين وواحد وعشرين ، في المنصة الإفتراضية للأكاديمية عبر فضائها الألكتروني.

ضّم العدد جمهرة كبيرة من البحوث لعلماء ولباحثين من جامعات عربية ، ولمؤسسات علمية ، ولمراكز بحثية متباينة في تخصصاتها المتنوعة على مدار الوطن العربي الواسع بجناحيه الآسيوي والأفريقي ، لذا جاء العدد على ثلاثة أجزاء ، يحتوي كل جزء منه على عدد من البحوث المتنوعة التي تشترك ضمن المحور الرئيس التنمية المستدامة.

إن الثقافة المستدامة يجب تبيانها عند جميع العاملين في منظمات القطاع الخاص ، عن طريق التعريف بها ، وتشجيع مبادئها ؛ لتحقيق أهدافها . وتفعيل ما يُعرف بالقطاع الثالث ، وهو القطاع الناتج عن الشراكة بين القطاعين ؛ العام ، والخاص ، للنهوض بعجلة التنمية وتحقيق أهدافها .وضرورة توفير رعاية علمية للباحثين في مجال العلوم الإنسانية والاجتماعية ، وتحقيق نُظُم المتابعة المثلى بما يكفل تحقيق الإبداع العلمي الخلاق .وتبني استراتيجية وطنية ، يشارك بها الخبراء من مختلف التخصصات التربوية ، والإعلامية ، والطبية ، لحماية الصحة العقلية للشباب عن طريق رفع مستوى الوعي لديهم ، وتوجيههم للاستعمال الرشيد لوسائل التواصل الاجتماعي المختلفة . وأهمية الإفادة من المناخ المحليّ ، وتوظيفه في تخطيط المدن ، وتصميم المباني ، وهو الجانب الفعال في تقليل استهلاك الطاقة ، والتفاعل الإيجابي مع مصادر الطاقة النظيفة ، التي وفرتها البيئة المحلية .وتطوير نُظُم إدارة المعرفة الرشيقة ، على أساس التكنولوجيا المتوافرة وتصميمها ؛ لتلبية احتياجات المنظمات الخدمية صغيرة الحجم ومتوسطها . والعمل على توفير بيئة سياسية وأمنية مستقرة ، تحفظ حقوق الإنسان الأساس ، وتلتزم بقيم العدل والمساواة .

وبعد هذا كُله.. وبموجز لما قاله المؤتمرون عبر بحوثهم .. يُعْدّ المؤتمر العلمي الدولي الثالث للأكاديمية الإفتراضي هو الأوسع نطاقا ليس في عدد المشاركات فحسب بل فيما تركه من استدامة علمية ومعرفية ، وقدرات أسْفر بها الباحثون عن فكر مستدام حر، وديمومة علمية إبداعية خلاقة . ونثمن بدورنا ذلك الجهد المضي والفعال من لدن كل مَنْ شارك ، وعمل ، وقدم لنجاح ذلك الصرح العلمي بامتداده الطويل . وستكون الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب المنبر الواسع لكل الأفكار التي تسهم في بناء حياة مستدامة خدمة لحياة الإنسان في ربوع أرضه العريقة .

ولاية ديلاوير 4 / 7 /2021 هيئة تحرير المجلة

الملاحظة القانونية

البحوث المنشورة في المجلة لا تعبر عن وجهة نظر المجلة ، بل عن رأي كاتبها .

فهرس الموضوعات

الأمن المعلوماتي: الجانب الدفاعي للذكاء الاقتصادي

د.فيلالي أسماء
جامعة أبوبكر بلقايد تلمسان– الجزائر–
filaliasma@outlook.fr
00 40 93 0669

الملخص

يهدف هذا البحث إلى دراسة جانب مهم من جوانب الذكاء الاقتصادي وهو الأمن المعلوماتي، والتعرف على أساليب تحقيق هذا الأخير في ظل البيئة الرقمية التي تشهد تطورا مستمرا، الأمر الذي ينتج عنه مخاطر وتهديدات جديدة ومختلفة يصعب التعامل معها بالأساليب التقليدية، بل يتطلب الأمر استراتيجية أمنية تغطي جميع الجوانب.

وتوصلت هذه الدراسة إلى أن العلاقة بين الأمن المعلوماتي والذكاء الاقتصادي علاقة طردية، وتعتمد نجاعة جهاز الذكاء الاقتصادي سواء على المستوى الكلي أو الجزئي على مدى تحقيق الأمن المعلوماتي، فالذكاء الاقتصادي منهج علمي جديد مادته الأساسية هي المعلومة الاستراتيجية، وتأمينها أمر ضروري في جميع مراحلها من بحث وجمع وتحليل وبث إلى غاية وصولها إلى أيدي متخذي القرار فتُتَخذ على أساسها قرارات استراتيجية تقدر فعاليتها بقدر فعالية المعلومة المستخدمة.

الكلمات المفتاحية: الذكاء الاقتصادي، الأمن الاقتصادي، الأمن المعلوماتي، البيئة الرقمية، التهديدات.

Information security: the defensive side of economic intelligence

Filali Asma

- University of Abu Bakr Belkaid Tlemcen - Algeria

Abstract

This research aims to study an important aspect of business intelligence, which is information security, and to identify ways to achieve it in the continued development of the digital environment, which brings new and different risks and threats that are difficult to manage in the traditional way, but it requires a security strategy that covers all aspects.

The study found that the relationship between IT security and business intelligence is progressive, and the efficiency of business intelligence service depends on the extent of IT security, as business intelligence is a new approach, whose main subject is strategic information, and its security is essential at all stages, from research, collection, analysis and transmission to decision-makers.

Keywords: business intelligence, Economic security, information security, Digital environment, threats.

مقدمة البحث

يشهد العالم اليوم تغيرات وتحولات جذرية في مجال الاقتصاد وفي علم الادارة كمنهج وأسلوب دون المساس بمبادئه الأساسية، وهذا بسبب التطور الهائل والسريع الذي شهده قطاع تكنولوجيا المعلومات والاتصال، حيث أصبحت الأجهزة الالكترونية قادرة على تحقيق الاتصال المباشر فيما بينها بغض النظر عن بعد المسافات، وهذا ما اعتبرته المؤسسات ميزة من الواجب استغلالها لتسريع المعاملات واختصار الوقت والجهد ومواكبة التطورات.

إن هذا التطور التكنولوجي ساهم وبدرجة كبيرة في تغيير طرق ووسائل تنفيذ الأنشطة الاقتصادية، ما أدى إلى ظهور نوع جديد في الاقتصاد يطلق عليه الاقتصاد الرقمي أو اقتصاد المعلومات، والذي تمثل فيه المعلومة الركيزة الأساسية للاقتصاد، فقد أصبحت جودة التعامل مع المعلومات المعيار الرئيسي لقياس قوة المنظمات، فمن يمتلك المعلومة في الوقت المناسب والمكان المناسب يمتلك القوة والسيطرة.

إن هذه البيئة الرقمية أو المعلوماتية التي تعمل في ظلها المؤسسات اليوم بقدر ما تعتبر قفزة نوعية في مجال الأعمال، بقدر ما تعتبر وسط خطير ومجال مناسب لظهور تهديدات ومخاطر من نوع جديد، وخطر هذه التهديدات يكمن في صعوبة اكتشافها واكتشاف مرتكبيها نظرا لحدوثها في عالم افتراضي ليس له حدود جغرافية وبالتالي تكون آثارها في أغلب الأحيان كارثية، وعليه في ظل هذا المحيط العدواني والمتداخل كان من الضروري ايجاد مناهج وآليات لحماية أنظمة المؤسسة ومعلوماتها الأساسية من الجرائم المعلوماتية الناتجة عن البيئة الافتراضية، ومن أهم المناهج التي اعتبرتها المؤسسات منهج استراتيجي ومتكامل في التعامل مع المعلومات الاستراتيجية **الذكاء الاقتصادي** الذي يرتكز ويسعى نحو تحقيق ثلاث أهداف رئيسية: تنافسية النسيج الصناعي، **أمن الاقتصاد والمؤسسات** وتدعيم التأثير.

مشكلة البحث

يرتكز الذكاء الاقتصادي على جانبين: جانب هجومي متمثل في اليقظة الاستراتيجية والتأثير، وجانب دفاعي متمثل في الأمن الاقتصادي وبالأخص الأمن المعلوماتي، ومن خلال هذا البحث سنبين أهمية الأمن المعلوماتي في الحفاظ على استمرارية المؤسسات في ظل التهديدات المستمرة، ودوره في تحقيق المعنى العام للذكاء الاقتصادي، مع التطرق لإستراتيجية الأمن المعلوماتي في المؤسسة من خلال معالجة الاشكالية التالية: **ما هي استراتيجية تحقيق الأمن المعلوماتي وما مدى مساهمة ذلك في تحقيق استراتيجية الذكاء الاقتصادي؟**

وللإجابة على هذه الاشكالية وجب أولا الاجابة على التساؤلات التالية:

- ما المقصود بالأمن المعلوماتي؟
- ما الفرق بين الأمن الاقتصادي والأمن المعلوماتي؟
- ما علاقة الأمن المعلوماتي بالأمن الاقتصادي والذكاء الاقتصادي؟
- ما استراتيجية تحقيق الأمن المعلوماتي في ظل البيئة الرقمية؟ وكيف يساهم ذلك في تحقيق الذكاء الاقتصادي؟

أهمية البحث

تكمن أهمية هذا البحث في كونه يتطرق إلى جانب من جوانب الذكاء الاقتصادي والذي غالبا ما يتم تجنب التطرق إليه وهو الأمن الاقتصادي على المستوى الكلي أو أمن المؤسسة على المستوى الجزئي، والذي ترتكز فكرته حول كيفية حماية الممتلكات غير المادية وأبرزها المعلومات في كل مراحل تداولها من مرحلة جمعها إلى غاية مرحلة بثها، إذ أنه غالبا ما يتم ربط الذكاء الاقتصادي باليقظة الاستراتيجية ودورها في تحقيق الميزة التنافسية مع تجاهل دور الحماية والأمن في تحقيق ذلك.

أهداف البحث

يهدف هذا البحث إلى تحقيق النقاط الآتية :

- إزالة اللبس الحاصل في التمييز بين المصطلحات الخاصة بالذكاء والأمن الاقتصادي.
- توضيح العلاقة بين الذكاء الاقتصادي والأمن الاقتصادي والعلاقة ببين الأمن الاقتصادي والأمن المعلوماتي.
- توضيح استراتيجية تحقيق الأمن المعلوماتي في البيئة الرقمية.

فروض البحث

- ترتكز استراتيجية الأمن المعلوماتي على تواجد أحدث البرمجيات والأنظمة.
- يصعب تحقيق عنصر السرية في الأمن المعلوماتي في عصر المطالبة بالشفافية والوضوح.

الدراسات السابقة

1. دراسة Tim Lane (2007) بعنوان: Information Security Management in Australian Universities-an exploratory analisis (إدارة أمن نظم المعلومات في الجامعات الاسترالية)

تهدف هذه الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الجامعات الاسترالية، والعوامل التي تؤثر على فاعليتها وكيفية تحسينها، وأجريت الدراسة على مستوى 38 جامعة استرالية، وخلصت إلى أن العوامل المؤثرة في فاعلية إدارة أمن المعلومات هي نقص الخبرات وضعف هيكلة إدارة أمن المعلومات، ضعف الوعي الأمني وعدم الاكتراث لخطر التهديدات، كما أن ضعف أو قوة إدارة أمن المعلومات مرتبط بمدى فاعلية العناصر البشرية باعتبارها الركيزة الاساسية للادارة الأمنية.

2. دراسة زكريا أحمد عمار (2011) بعنوان: حماية الشبكات الرئيسية من الاختراق والبرامج الضارة

تمثلت اشكالية هذا البحث في التساؤل التالي: **ما هي طرق ووسائل حماية موارد شبكات الحاسب الآلي؟** وتهدف هذه الدراسة إلى تحديد وسائل وإجراءات حماية الشبكات الرئيسية ومصادر المعلومات الموجودة فيها أو المنقولة منها على مستوى المؤسسات التعليمية بمدينة الرياض بالمملكة السعودية، وخلصت الدراسة إلى أن مشكلات حماية وتأمين موارد شبكات الحاسب الآلي، لا تكمن في توريد وتثبيت الأجهزة والبرمجيات فقط، وإنما في توفير وإعداد الانسان القادر على ادارة وتشغيل تلك الأجهزة والبرمجيات. ولعدم وجود توافق بين الهياكل التنظيمية وإجراءات ووظائف الموارد البشرية العاملة في مجال الحماية بالعينة المدروسة، فان الوصول إلى حماية أفضل لشبكات الحاسب الآلي تتطلب إعادة تصميم الهياكل التنظيمية، وللتغلب على صعوبات الحماية لابد من توفير أخصائيين في أمن المعلومات، وتوفير عدد كافي من موظفي أمن المعلومات يحملون مؤهلات علمية تتناسب مع متطلبات أعمال الحماية وتوفير مسميات وظيفية مع بيان المهام والواجبات.

3. دراسة نهاد عبد اللطيف ود.خلود هادي الربيعي (2013) بعنوان: أمن وسرية المعلومات وأثرها على الأداء التنافسي

عالجت هذه الدراسة اشكالية **مدى تأثير أمن وسرية المعلومات على الأداء التنافسي لشركات التأمين**، وتوصلت إلى نتائج معينة كانت من أهمها وجود علاقة ارتباط وتأثير بين أمن وسرية المعلومات والأداء التنافسي لشركات التأمين.

4. دراسة **Christophe Guillou** و **Alain Marcay** (2015):

Etude prospective et stratégique: Réseaux internet et sécurité

تهدف هذه الدراسة إلى إجراء تحليل مستقبلي إلى غاية عام 2030 للأمن السيبراني لشبكة الإنترنت المدنية، لا سيما على المستوى التقني، ولكن أيضا على الصعيد الاجتماعي والتنظيمي والقانوني والاستخدامات، ومن بين توقعات الدراسة أن الثورة القادمة بحلول 2030 ستكون حول:

- انترنت الآلات وبالتحديد (آلة مقابل آلة) ففي الواقع، لن تكون شبكة الإنترنت مجرد ناقل للاتصال بين الأفراد والآلات، بل بين آلات مستقلة تماماً وذكية بشكل متزايد .
- بخصوص الشبكات ذات الكفاءة المتزايدة، فإن اتساع نطاق الأجهزة وخاصة البرمجيات، سواء في المجال المهني أو عامة الناس، سيوسع نطاق الهجمات الإلكترونية وشدتها؛ وفي هذا السياق الجديد المعايير الأمنية ستتغير وستصبح أكثر تعقيدا.

5. دراسة قدايفة أمينة (2016) بعنوان: استراتيجية أمن المعلومات

تم معالجة الموضوع تحت ضوء الاشكالية التالية: **كيف يمكن تبني استراتيجية أمنية ضرورية لحماية أمن المعلومات في المنظمة؟**، وتهدف هذه الدراسة إلى التأكيد على أن أهمية أمن المعلومات للمنظمات هي حاجة ضرورية، وخلصت الدراسة إلى أن أمن المعلومات يحتاج إلى استراتيجية قوية، بهدف حماية البنية التحتية ومواجهة التهديدات، وهذه الاستراتيجية تتطلب متابعة ومراجعة بشكل دوري للتأكد من ملائمتها للتغيرات.

6. دراسة رؤى يونس (2017) بعنوان: دراسة واقع ادارة أمن نظم المعلومات في المؤسسات السورية

تهدف هذه الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في وزارة الاتصالات و التقانة والجهات المرتبطة بها، واستخدمت الباحثة في دراستها المنهج الوصفي التحليلي، وخلصت الدراسة إلى أن الادارات العليا للوزارة والجهات المرتبطة بها تدرك أهمية سياسات أمن المعلومات إلا أنه لا يوجد في أي من الجهات سياسات معمول بها ومطبقة على أسس واضحة .

منهج البحث

تم الاعتماد في هذا البحث على المنهج الوصفي التحليلي، لوصف مختلف المفاهيم التي أنتجتها البيئة الرقمية مثل الذكاء الاقتصادي والأمن المعلوماتي، وتحليل العلاقة بين تحقيق الأمن المعلوماتي وتحقيق الذكاء الاقتصادي، وطرق الأمن المعلوماتي في مواجهة التهديدات الناتجة عن البيئة الرقمية.

المحور الأول:العلاقة بين الأمن المعلوماتي والذكاء الاقتصادي

على الرغم من أن المبادرة والتدابير الهجومية هي من أولويات معظم الأعمال المتعلقة بالذكاء الاقتصادي إلا أن الجانب الدفاعي لهذا الأخير لا يمكن تجاهله، فباعتبار أن الذكاء الاقتصادي منهج قائم بذاته على المعلومة المفيدة والفعالة فان تأمينها هو الأولوية الأساسية من أجل اتخاذ قرارات فعالة.

1. ماهية الذكاء الاقتصادي والأمن المعلوماتي

قبل توضيح العلاقة بين الأمن المعلوماتي والذكاء الاقتصادي يجب أولا التعرف على هذين المفهومين وذكر عناصرهما.

1.1 الذكاء الاقتصادي

إن الذكاء الاقتصادي نهج نابع من الفكر العسكري، الذي يعتمد على المعلومة من أجل اكتشاف نقاط قوة وضعف الخصم، ومن ثم تحليلها من أجل الاستعداد الجيد لمواجهته، هذا التطور المعلوماتي في المجال العسكري أدى تدريجيا إلى خلق خلايا خاصة ب"الذكاء التسويقي" داخل المؤسسات، وأصبح علم معتمد مثله مثل أي علم آخر من علوم التسيير. (Martre, 1994, pp. 23-25)

لقد تعددت تسميات الذكاء الاقتصادي منذ ظهوره، فمن الذكاء التنافسي إلى ذكاء الأعمال إلى الذكاء التنظيمي، إلى غاية سنة 1994 أين كان أول تعريف عملي للذكاء الاقتصادي في فرنسا من خلال تقرير المحافظة العامة للتخطيط "الذكاء الاقتصادي واستراتيجية المؤسسات" الذي ترأسه Henri Martre .

وعرف Henri Martre الذكاء الاقتصادي على أنه "مجموعة الأعمال المرتبطة بالبحث، معالجة، وبث المعلومة المفيدة للأعوان الاقتصاديين، مختلف هذه النشاطات موجهة بطريقة شرعية مع توفير كل ضمانات الحماية الأساسية لممتلكات المؤسسة في ظل أحسن الظروف سواء من حيث الوقت، الجودة أو التكلفة" (Martre, 1994, p. 11)

فبالتالي نفهم من هذا التعريف أن المعلومة يجب أن تكون محمية بمجموعة من الضمانات في جميع المراحل التي تمر بها من بحث وتحليل وبث.

وعرف "Alain Juillet" المسؤول الأعلى للذكاء الاقتصادي بفرنسا الذكاء الاقتصادي على أنه "أسلوب تحكم يعمل على السيطرة وحماية المعلومة الاستراتيجية لكل الأعوان الاقتصاديين من أجل الوصول إلى المنافسة، الأمن الاقتصادي وأمن المؤسسات."(Legendre, 2006, p. 5)

أي أن الذكاء الاقتصادي أسلوب يحقق الأمن الاقتصادي عن طريق التحكم الجيد في المعلومة الاستراتيجية.

2.1 الأمن المعلوماتي

بدأت المؤسسات تهتم بالأمن المعلوماتي بداية الثمانينات، وفي بداية التسعينات ظهر مصطلح أمن أنظمة المعلومات الذي لم يقتصر على مسائل البنية التحتية بل حماية أنظمة المعلومات الحساسة بطريقة مختلفة، فالحاجة إلى الأمن لا تقتصر في مصطلح الاتاحة فقط وانما في مصطلح السرية والتكامل أيضا. (Matthieu Bennasar, 2007, p. 13)

ويتمثل الأمن المعلوماتي بصفة عامة في ضمان أن الموارد المادية والبرمجية للمؤسسة مستعملة فقط في الاطار المحدد لها، فهو يضمن حقوق الوصول للمعطيات وموارد النظام عن طريق ميكانيزمات التحقق من الهوية والمراقبة، وهذا يعني أن المستخدمين يمتلكون ويعملون فقط في حدود الحقوق الممنوحة لهم. فمن الضروري أن يضمن الأمن المعلوماتي عدم إعاقة هؤلاء المستخدمين من أداء وظائفهم الضرورية وتطويرها وضمان قدرتهم على استخدام النظام بكل موثوقية. (Godart, 2005, p. 15)

وفي النطاق العام الأمن يجب أن يُضمن على المستويات التالية (ACISSI, 2009, p. 12):

- على مستوى المستخدمين: الأعوان عليهم معرفة أهمية مواقعهم.
- على مستوى التكنولوجيا المستخدمة: يجب أن تكون مضمونة ولا تقدم ثغرات يمكن استغلالها.
- على مستوى المعطيات، مع تسيير جيد لحقوق الوصول (المستخدم يجب أن يمتلك حقوق الوصول الضرورية لعمله فقط).
- على المستوى المادي: لا يفيد أبدا حماية نظام منطقيا إذا كان الوصول المادي للآلات ليس مؤمنا.

ويغطي الأمن المعلوماتي أربعة أهداف أساسية، تمثل على شكل (C.I.D.P) (Carpentier, 2009, p. 13)

- **السرية** (Confidentialité):وهي ضمان وصول المعلومة للأشخاص المعنيين فقط ولا تنتشر خارج المحيط المخصص لها.
- **التكامل** (Intégrité): وهي ضمان وجود المعلومة دون تعديل أو تخريب.
- **الاتاحة** (Disponibilité) وهي ضمان وصول المستخدمين المعنيين للمعلومات التي يطلبونها في الوقت المحدد لمعالجتها.
- **الدليل** (Preuve): تتمثل في ضمان أن مرسل المعلومات معرف جيدا وله حقوق الدخول المنطقي، وأن المستقبل المعرف مسموح له الوصول للمعلومة.

2. الأمن المعلوماتي ركيزة أساسية في تحقيق الذكاء الاقتصادي

يتكون الذكاء الاقتصادي من ثلاث عناصر رئيسية: اليقظة، الأمن الاقتصادي أو أمن المؤسسات، التأثير، حيث يمثل الأمن الاقتصادي الجانب الدفاعي للذكاء الاقتصادي، والأمن الاقتصادي هو مفهوم يطبق على المستوى الكلي، أما على المستوى الجزئي فالأمر يتعلق بأمن المؤسسة الذي يتحقق بتحقيق أمن المعلومات نظرا للتطور الذي عرفته نظم المعلومات وتطور المخاطر المتعلقة بها.

1.2 الأمن الاقتصادي جزء من الذكاء الاقتصادي

1.1.2 تعريف الأمن الاقتصادي

نتيجة للتطورات الاقتصادية والتكنولوجية الأخيرة، وتلاشي كل أنواع الحواجز بين البلدان ليصبح العالم سوقا واحدا، زادت التحديات وزادت المخاطر التي أصبح من الصعب التحكم فيها بصفة كاملة، خاصة الجوسسة الاقتصادية أو التجسس الاقتصادي أو الصناعي بين البلدان، ما جعل الأمن الاقتصادي ضرورة حتمية للدولة من أجل البقاء في هذا السوق الموحد وليس خيارا يمكن التفكير فيه.

الأمن الاقتصادي هو تجسيد لسياسة دولة من أجل حماية وترقية المصالح الاستراتيجية للدولة، ففي جانبه الدفاعي يتضمن النشاطات التالية: حماية الممتلكات والارث المعلوماتي والتكنولوجي للمؤسسات والسلطات العمومية، تحديد المحيط الصناعي

والتكنولوجي الخطر، المقاومة ضد نشاطات الاستعلام الاقتصادي الأجنبية، أما جانبه الهجومي يتمثل في مرافقة التطور الى العالمية.
(centre national de ressources et d'information sur l'intelligence économique et stratégique, 2014)

ومن خلال هذا التعريف يتضح أن الأمن الاقتصادي سياسة متكاملة هدفها حماية الدول والمؤسسات من التعديات الخارجية، وتشمل الحماية الإرث المادي والإرث المعلوماتي.

الأمن الاقتصادي هو الاعتماد في نفس الوقت على استراتيجية قانونية(ايداع براءات الاختراع، حماية الماركات...) وعلى الأمان(معايير حماية المعرفة الاستراتيجية من خلال أنظمة المعلومات، تحسيس أفراد المؤسسة، ملاحظة تجارب وتصرفات المنافسين...) اضافة إلى انتباه المؤسسة للواجب القانوني في حماية مستخدميها والتيقظ على أن المعلومات الخاصة بهم محمية ومؤمنة والفهم المعمق لشروط المنافسة .(Gloaguen, 2014, p. 40)

2.1.2 علاقة الأمن الاقتصادي بالذكاء الاقتصادي

الذكاء الاقتصادي هو مجموعة نشاطات مترابطة ومتناسقة تتمثل في: البحث، المعالجة، بث وتقييم وحماية المعلومة المفيدة، ويرتكز الذكاء الاقتصادي على ثلاث محاور رئيسية.(Pardini, 2009, p. 3) :

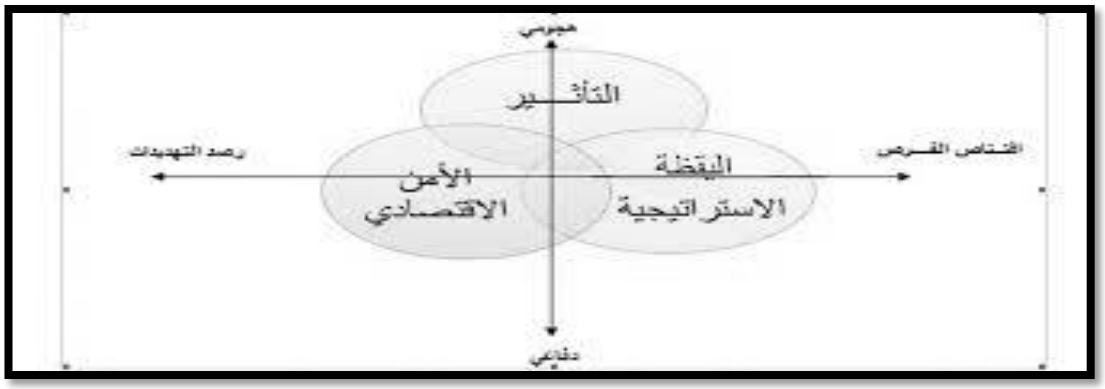
- تطوير وتجنيد قدرات اليقظة الاستراتيجية التي تسمح للأعوان السياسيين والاقتصاديين بتفسير التغيرات التي يعيشونها.
- الترويج لنموذج تطوير اقتصادي، اجتماعي وثقافي يعطي ميزة تنافسية للقطاع.
- تفعيل استراتيجية أمن اقتصادي ترتكز على تعريف نطاق الممتلكات المفتاحية في القطاع، هذه الممتلكات يجب أن تكون محمية والاستفادة كذلك من دعم يعزز تطورها، ومن هنا سياسة أمنية اقتصادية ستشمل أيضا نشاطات التأثير يجب أن تكون في تناسق عام مع النشاطين الآخرين.

الأمن الاقتصادي إذن هو عنصر غير منفصل عن كل جهاز ذكاء اقتصادي، وحسب Sylvianne Descharmes المسؤول عن اليقظة الصناعية على مستوى l'ARIST[1] فان الذكاء الاقتصادي يتمحور حول ثلاث عناصر:

- **اليقظة**: وهي المراقبة المستمرة لمحيط المؤسسة من أجل التوصل إلى المعلومات المطلوبة قبل الآخرين من أجل اتخاذ أحسن القرارات.
- **الأمن**: ويعرف الأمن الاقتصادي عموما على أنه تأمين الممتلكات المعلوماتية للمؤسسات والسلطات العمومية.
- **التأثير**: يتمثل في الضغط على مجموعة من الأعوان لفائدة المؤسسة من أجل أن تكون أكثر قدرة على تحقيق أهدافها الإستراتيجية أو من أجل إيقاف التهديدات التي يمكن أن تواجهها.

[1] l'ARIST: الوكالة الاقليمية للمعلومة الاستراتيجية والتكنولوجية

الشكل1: مكونات الذكاء الاقتصادي



Source: (Clerc, 2013, p. 4)

2.2 الأمن المعلوماتي جزء من الأمن الاقتصادي:

الأمن الاقتصادي هو مفهوم كلي يطبق على مستوى الدول، أما على المستوى الجزئي فالأمر يتعلق بأمن المؤسسة الذي يعتبر جزء لا يتجزأ من الأمن الاقتصادي، ويتمثل أمن المؤسسة في:

- **أمن موقع المنظمة:** أمن المنظمة يعني تحقيق الأمن المادي لموقع المنظمة والسيطرة الخارجية للبناية وحمايتها من كل تدخل طبيعي أو متعمد، وهذا يعتبر كخطوة استباقية لضمان وحماية نشاط المؤسسة واستمرارها.
- **أمن تجهيزات نظم المعلومات:** ويتمثل في حماية قاعات المعلوماتية من الكوارث الطبيعية والحوادث ومراقبة الدخول غير المرخص إليها.
- **الأمن المعلوماتي:** أو ما يسمى بالحماية البرمجية لنظم المعلومات ويتعلق الأمر هنا بتوفير الحماية التامة للمعلومات الاستراتيجية ليس فقط حماية تواجدها وإنما يتعلق الأمر أيضا بسريتها وتكاملها أيضا.

وعليه فان الأمن المعلوماتي هو جزء من أمن نظم المعلومات أو أمن المؤسسة لأن الأمن المعلوماتي يتعلق بحماية المعلومات على مستوى أجهزة الاعلام الآلي أو المعلوماتية، أما أمن نظم المعلومات فهو عبارة عن حماية المعلومات بصفة عامة سواء على مستوى وسائل المعلوماتية أو خارجها وتكون الحماية مادية وبرمجية وبشرية لذا يسمى بأمن المؤسسة بصفة عامة.

3.2 الأمن المعلوماتي جزء من الذكاء الاقتصادي

المعلومة هي قلب كل جهاز ذكاء اقتصادي، فهي منتج خاص تزيد قيمته بفضل مشاركتها وتناقلها، مع العلم أنه بمجرد بثها تفقد المعلومة قيمتها السوقية، فالمفارقة تكمن في كيفية تحقيق معادلة بث المعلومة مع حمايتها والحفاظ على سريتها في نفس الوقت، وهذا ما يجعل من تفعيل جهاز الذكاء الاقتصادي أمرا صعبا، ومن هنا تأتي فكرة "التحكم في المعلومة" من أجل وصولها لمتخذي القرار في وقت قياسي واستخدامها بفعالية، وهذه مهمة الأمن المعلوماتي وأعوان الأمن الذين عليهم ضمان بث المعلومة المفيدة سواء في الأوقات العادية أو في الأزمات من أجل تمكين متخذي القرار من تكوين واعطاء الأوامر الضرورية في الوقت المناسب. (Pardini, 2009, p. 7)

وترتكز عملية التحكم في المعلومة على 3 أساسيات.(Pardini, p. 7) :

- توافقية شبكات المعلومة التي تسهل دوران المعلومة.
- حماية المعلومة أو أمن أنظمة المعلومات التي تسمح بضمان سرية، توافر، تكامل النظام والمعلومة المعالجة.
- التحقق من المعلومة، دقتها، دورانها الجيد وقيمتها.

المحور الثاني: الأمن المعلوماتي: ضمان البقاء في ظل البيئة الرقمية

حسب دراسة في الولايات المتحدة من طرف National Archives and Records Administration في 2018 فان 93% من المؤسسات فقدت بياناتها خلال 10 أيام أو أكثر أعلنت افلاسها في سنة الكارثة، و50 % أو دعوا ميزانياتهم مباشرة بعد الهجمة.(Fréminville, 2019, p. 8)

هذه الأرقام تدل على خطورة الأمر وضرورة ايجاد الطرق والأساليب الفعالة من أجل ضمان البقاء في ظل هذه البيئة المحفوفة بالمخاطر، وهذا لا يتحقق إلا بصياغة استراتيجية متكاملة لتحقيق الأمن المعلوماتي.

1. البيئة الرقمية في المؤسسة

مع تطور تكنولوجيا المعلومات والاتصال، بدأت المؤسسات تتخلى شيئا فشيئا عن أنظمة المعلومات التقليدية وتنتقل من العمليات المادية إلى العمليات اللامادية المعتمدة على البيانات والمعطيات الموجودة على الأجهزة المعلوماتية، بمعنى آخر المؤسسات رقمنت كل عملياتها سواء المالية(محاسبة، محاسبة تحليلية، علاقات البنك، تسيير الخزينة) أو علاقاتها مع الأطراف المعنية(الموردين، الزبائن، المساهمين، موردي الخدمات)، إضافة إلى رقمنة تسيير الموارد البشرية (الرواتب، التوظيف، التكوين)، والتواصل الداخلي والخارجي خاصة مع انتشار وسائل التواصل الاجتماعي. (Fréminville, p. 9)

تقيم المؤسسة عادة على أساس كفاءتها المالية (حساباتها، نتائجها، ميزانيتها، خزينتها،معدل نموها...)، ولكن ماذا عن كفاءتها الرقمية؟ تسيير المعطيات، أمن المعطيات (تكامل، سرية، توافر)، حماية أنظمة المعلومات التي تسمح بتبادل، تخزين وتعديل المعطيات؟ إذ يمكن أن تكون المؤسسة كفأة ماليا، ولكن خسارة في أنظمتها المعلوماتية أو أمنها الرقمي يمكن أن يمس بشكل كبير قدرتها على البيع، الانتاج، الدفع للموردين..وبالتالي التراجع في نتائجها المالية، سمعتها، ثقة المساهمين والأطراف الفاعلة. (Fréminville, p. 10)

وبالتالي لعبت المعلوماتية دورا أساسيا في تطور العديد من الخدمات والمجالات، ولكن لا يمكن النجاح في ذلك إلا في ظل بيئة آمنة، فالأمن المعلوماتي هو في قلب إشكالية المعلوماتية سواء الكلية أو الجزئية.

2. مخاطر البيئة الرقمية

مخاطر التهديدات المعلوماتية ترافق تطور الأنظمة الرقمية وخاصة المتصلة بالانترنت، من الضروري جدا على المؤسسة تعريف التهديدات التي قد تواجهها وإلا فان أي ثغرة يمكن أن تكلف المؤسسة خسائر جسيمة.

1.2 تعريف مخاطر وتهديدات البيئة الرقمية

تهديدات الأمن المعلوماتي هو مصطلح حديث نوعا ما ظهر بظهور الاعلام الآلي والحواسيب، وانتشر بتوسع استخدامها وتطور خدماتها، فكلما زادت فوائد هذه الأنظمة وزاد الاعتماد عليها،زادت التهديدات عليها.

في مجال الاعلام الآلي، يعرف التهديد "كنشاط أو حدث بمجرد إطلاقه يمكن أن يحدث إصابات على أحد أو كل الخصائص الحرجة للمعلومة والأنظمة التي تحملها وتحفظها وهي السرية، التكامل والإتاحة والتوافر". (Godart, 2005, p. 51) ويعرف أيضا على أنه "حدث أو جهة تشوش نظام المعلومات عن طريق استغلال ثغرة من أجل الحصول، تعديل أو إعاقة الوصول لأصل من الأصول أو تعريضه للخطر، ويتلخص في الأخطاء الإرادية وغير الإرادية، الاحتيال، النشاطات المحتملة من العمال الخبيثين، الحوادث والأسباب الطبيعية، الهاكر، البرامج الخبيثة". (Carpentier, 2009, pp. 23,31)

وعليه التهديد هو أي خطر محتمل للمعلومات أو الأنظمة التي تحويها أو بصفة أخرى هو كل تصرف يمكن أن يؤثر سلبا على سرية، تكامل وتوافر المعلومات.

2.2 أنواع مخاطر البيئة الرقمية

مخاطر البيئة الرقمية عديدة ومتعددة يمكن حصرها في 3 أشكال رئيسية: القرصنة المعلوماتية والبرامج الضارة والثغرات الأمنية.

1.2.2 القرصنة المعلوماتية

"القرصنة تعمل على كشف نقاط ضعف نظم الحماية لمواقع الانترنت والأنظمة المعلوماتية، وغالبا ما يتم استغلال مختلف وظائف الانترنت التي تحوله إلى نظام مفتوح سهل الاختراق".(Laudon & Laudon, 2006, p. 354)

وعليه هذا النوع من تقنيات الاعتداء يتمثل في محاولة اقتحام أنظمة المعلومات والحصول على المعلومات السرية بأي طريقة، ومن أشهر طرق القرصنة المعلوماتية:

- **التنصت**

التنصت يكمن في "التموقع على شبكة معلوماتية أو شبكة التواصل عن بعد، ومن ثم تحليل وتخزين المعلومات العابرة، وترجمة التآمرات وكل ما يدور داخل الشبكة المعلوماتية". (Guide N65, 2006, p. 13)

ومن الأدوات المستخدمة لتنفيذ التنصت برامج تحليل الشبكات وبروتوكولاتها كبرنامج "Sniffer" فهذا البرنامج التجسسي يسمح بالتنصت على الحركة على الشبكة المعلوماتية التي تتصل مباشرة بالحاسب، ومن أولوياته البحث عن تحديد الحزم التي تضم كلمات login أو password. (Léopold & Lhoste, 2007, p. 53)

- **رفض الخدمة**

"هي نشاط خبيث يترجم بعدم اتاحة مؤقت أو دائم لمكونات نظام الاتصال عن بعد". (Lafitte, 2003, p. 88)
ومن أشهر طرق تطبيق هذه الهجمة **فيروس bot**: هذا الفيروس لا يعمل سوى أنه ينتشر، ولكن في ساعة محددة أو إشارة معطاة آلاف أو ملايين الآلات المصابة تتصل بنفس الخادم المستهدف وتثير انهياره. (Vaucamps, 2010, p. 14)
كما يطلق عليه اسم شبكة الروبوتات أو البوت نت (botnets) ويتمثل خطرها في سيطرة شخص أو مجموعة يعرف بالمتحكم (Master) على شبكات ضخمة من الأجهزة الحاسوبية ربما يبلغ عددها الآلاف بل حتى الملايين، ويمكن لذلك المتحكم أن يطلب من تلك الأجهزة القيام في توقيت محدد عن طريق برنامج تحكم يطلق عليه برنامج السيطرة والتحكم بتنفيذ أوامر معينة لأغراض تجارية أو تخريبية، وتتم كل هذه الأمور بشكل خفي ومن الصعب جدا اكتشافها من مستخدمي الأجهزة **(العزب، 2018، صفحة 14)**

- **سرقة الهوية**

سرقة الهوية أو التنكر هو من أنواع السبل غير الشرعية، تتعلق بهجمة معلوماتية تكمن في انتحال هوية شخص آخر والاستفادة من امتيازاته وحقوقه عن طريق اغتصاب هويته، وأهم تقنية خداع مستعملة هي هجمة مسماة "par spoofing"تسمح لهيئة ما أن تكون مشابهة لتلك الأصلية عن طريق بريد مظهره يوحي أنه عنوان موثوق بهدف الوصول خفية إلى تطبيقات ومعلومات حساسة. (Lafitte, 2003, p. 85) بمعنى هؤلاء القراصنة يقومون إما بخلق موقع مزور مشابه، أو ارسال رسائل الكترونية يبدو عنوانها المرسلة منه هو ذلك الخاص بالمنظمة الحقيقة أي لا مجال للشك فيه، ويطلب منك في هذه الرسائل إما الموافقة على ملف أو تحديث بيانات أو الموافقة على إجراءات جديدة للحماية عن طريق إدخال رقم بطاقة الائتمان أو كلمة مرور أو رقم بطاقة الضمان الاجتماعي، وعليه تكون قد وضعت المعلومات السرية والثمينة في موقع مزور.

2.2.2 البرامج الضارة: مثل الفيروسات والديدان المعلوماتية، حصان طراودة والقنابل المنطقية.

- **الفيروسات**

اليوم نشاط الفيروس لم يعد محصورا في إعادة النسخ وإطلاق الهجوم بل هناك نشاط إضافي يجب أخذه بعين الاعتبار وهو ضمان بقائه، إذ أصبح الفيروس يخفي تواجده باختلاطه مع ملفات ضرورية لعمل الأنظمة، وفي نفس السياق ولزيادة تعقيد اكتشاف الفيروس ظهر مؤخرا ما يسمى ب polymorphisme وهي قدرة الفيروس على أخذ عدة أشكال من أجل تضليل برامج مكافحة الفيروس إضافة إلى ظهور ورشات خلق برامج فيروسات يسمح بإضافة على الفيروسات الموجودة قدرات تشفير ليصبح تحديدها أكثر تعقيدا. (Léopold & Lhoste, 2007, p. 42)

- **الديدان الالكترونية**

بالنسبة لتحقيق الدودة فهو أمر صعب ولكن بمجرد النجاح في ذلك تحدث خسائر كارثية، وأكبر دليل هو الدودة المعروفة تحت اسم Slammer وهي أشهر دودة عبر التاريخ، ففي 25 جانفي 2003 انتشرت الدودة عبر الانترنت وأصابت أكثر من 90% من أنظمة المعلومات العالمية في 10 دقائق.

- **حصان طراودة**

ببساطة يمكن أن يبعث لك شخص خبيث بريد يقول فيه: "مرحبا، كيف حالك، أنظر إلى هذا الملحق" وعند فتحه تجد لعبة أو رسوم متحركة تبدأ تنشط، وعندما تكون تمضي وقتا ممتعا، حصان طراودة يكون يستقر في أحشاء الحاسوب ليسيطر عليه، فهذا النوع من الرموز يسمح برؤية ضربات لوحة المفاتيح، رؤية الشاشة بأكملها، اطلاق برامج بدون علم المستخدم، الوصول إلى معلومات مخزنة في القرص الصلب وكذلك شبكة المنظمة التي يتصل بها المستخدم، ويمكن أيضا التصنت على المحادثات وفقد السيطرة على لوحة المفاتيح. (Godart, 2005, p. 65)

3.2.2 الثغرات الأمنية

تعرّف الثغرة الأمنية على أنها نقطة ضعف في تصميم أو تهيئة البرمجيات أو قواعد تخزين المعلومات أو الأجهزة التي تحفظ فيها المعلومات، أو معدات أو برامج تشغيل الشبكات التي تمر المعلومات خلالها، ونقاط الضعف هذه هي الثغرات التي يتسلل المهاجم من خلالها لإحداث الدمار الذي يريده. (الغثبر و القحطاني، 2009، صفحة 24) وتتمثل غالبا في:

- **أخطاء البرمجة:** أخطاء البرمجة والثغرات الأمنية على مستوى البرامج تسمح بالتعدي على النظام والوصول إلى المعلومات السرية وبالتالي اختراق النظام، مما يسمح بتنفيذ وشنّ مختلف الهجمات، هذه الأخطاء تسبب ضياع انتاجية غير محددة، فحسب NIST[1] لمديرية التجارة للولايات المتحدة فان أخطاء البرامج تكلف كل سنة كثيرا الاقتصاد الأمريكي. (Laudon & Laudon, 2006, p. 357)
- **سوء إدارة المواقع:** القراصنة يبحثون بانتظام عن المواقع سيئة الادارة باستعمال مسح على الانترنت عن طريق تطبيقات تسمى "scan"، هذه التطبيقات تكشف عن بعد كل محطات الشبكة المحلية وتفحص وجود "الطبعات القديمة" للبرامج الشبكية على هذه المحطات مع فجوات أمنية معروفة. (Longeon & Archimbaud, 1999, p. 12)
- **استخدام عنوان انترنت دائم:** عندما تكون شبكة المؤسسة متصلة مع الانترنت، فأنظمة معلوماتها تصبح أكثر حساسية للتدخلات الخارجية، فالحواسب المتصلة دائما بالانترنت هي أكثر عرضة للتدخلات لأنها تستعمل عنوان انترنت دائم يسهل تعارفاتهم، فعنوان انترنت دائم يهدي القراصنة هدف ثابت.(Laudon & Laudon, 2006, p. 349)
- **سوء استخدام الرسائل الالكترونية:** الاستعمال المنتشر للبريد الالكتروني والرسائل الفورية تزيد من حساسية نظم المعلومات، فهذه الرسائل يمكن أن تكون معرّضة للقراءة من قبل دخلاء خلال ارسالها بالانترنت. (Laudon & Laudon, p. 350)
- **تعقد القواعد على الجدران النارية والمحركات:** وضع التصفيات وقواعد الوصول بالطلب تجعل رؤية الجميع شبه مستحيلة.
- **عدم وجود تحديثات لأنظمة التشغيل والتصحيحات،** وعدم وجود مراقبة كافية للبرامج الخبيثة، إضافة إلى اهمال الاهتمام بطرق الحماية من الاختراق، واهمال تحديث برامج مكافحة الفيروسات.

3.2 استراتيجية تحقيق الأمن المعلوماتي في المؤسسة

[1] NIST: National Institute of Standard and Technology.

تحقيق أمن المعلومات داخل المؤسسة يتطلب دراسة شاملة لكل الجوانب، وخطة استراتيجية محكمة تتمثل أولا في دراسة المحيط والأصول الواجب حمايتها مع تحديد مستوى الأمن الحقيقي الذي تقف فيه المؤسسة من أجل تحديد الطريق الواجب اتخاذه، ومن ثم تطبيق اجراءات الأمن المناسبة، لأن أمن المعلومات ليس وصفة يمكن اتباعها من قبل الجميع بل لكل مؤسسة خصوصيتها وأسلوبها.

1.3.2 تحديد الأصول الواجب حمايتها

"كل منظمة راغبة في حماية أنظمتها وشبكاتها يجب أن تحدد نطاق الأمن الذي يشمل الهيئات المادية وغير المادية" (Bloch & Wolfhugel, 2011, p. 10) هذه الهيئات خصوصا غير المادية تمثل البنية التحتية التي بدونها لا يمكن أن تتواجد نظم المعلومات، "اتاحة هذه البنية التحتية يجب أن تكون محمية، وتشمل: الخوادم، الشبكات، قواعد المعطيات، محطات العمل، البرامج". (Bloch & Wolfhugel, 2009, p. 210). وأهم خطوة في تحديد الأصول والنطاق هو تصنيف المعلومات وتحديد المعلومات الحساسة، هذه العملية كما أنها الحجر الأساسي لبناء سياسة أمنية إلا أنها يمكن أن تمثل نقطة ضعف سياسة الحماية لأنها عملية معقدة وخطرة، إذ يمكن أن تقود المؤسسة إلى درجة نسيان الهدف الذي هو: حماية المعلومات الضرورية والحرجة للمؤسسة، وهذا إذا تم الخوض فيها أكثر من اللازم.(Rouhier, 2008, p. 17) .

ولتقييم وتصنيف مدى سرية وحساسية المعلومات بالمنشأة، ولتحديد نوع ودرجة الحماية الأمنية فان المحددات الممكن اعتمادها هي: فائدة المعلومات، أهمية وقيمة المعلومات، عمر المعلومات، حجم الخسائر التي قد تلحق بالمنشأة عند كشف المعلومات أو عند حدوث تعديل أو تلف بالمعلومات، القوانين واللوائح والمسؤوليات الخاصة بحماية المعلومات، مدى تأثر الأمن بهذه المعلومات، من المصرح له باستخدام المعلومات، من الذي سيقوم بصيانة المعلومات، أين ستحفظ المعلومات، أي نوع من المعلومات يحتاج إلى تصنيف خاص. (المركز القومي للمعلومات، 2010، صفحة 9)

2.3.2 تحديد مستوى الأمن:

لمعرفة المستوى الحقيقي لأمن نظم المعلومات يقوم مسؤول أمن المعلومات بالتعرف على أعوانه الأساسيين لتكوين رؤية مناسبة للمنظمة ونظم المعلومات، ويطلب من كل واحد حسب نشاطه وكفاءته تحديد التطبيقات المطبقة في مجال الأمن، بعد هذا كله يكون لديه العناصر الكافية لتحرير "التقرير"، بمعنى وثيقة توضح الثغرات الأمنية في كل جانب من نظام المعلومات، هذه الوثيقة تحدد المستوى الحقيقي لأمن نظم المعلومات.(Fernandez-Toro, 2016, p. 5)

ويمكن عموما تقسيم مستويات الأمن إلى ثلاثة مستويات(Fernandez-Toro, pp. 6-10) :

أ- **منطقة الهوان:** هو المستوى الذي نجد فيه العديد من الثغرات المعروفة وسهلة الاستغلال من قبل المهاجمين ما قد يسمح لهم بالسيطرة الكلية على نظم المعلومات، ما يؤدي إلى نتائج كارثية على المؤسسة. نظم المعلومات المتواجدة في "منطقة الهوان" تعتمد عموما إجراءات حماية أولية مثل: كلمات المرور، برامج مكافحة الفيروسات، الجدران النارية، والإجراءات الأمنية غالبا تتوقف هنا.

ب- **مستوى الأمن الأساسي:** هذا المستوى أعلى وأحسن من منطقة الهوان، ويسمح لنظام المعلومات الصمود في وجه الهجمات متوسطة الخطورة، ولكن الاصابات الخطيرة على نظام المعلومات تبقى ممكنة.

ت- **مستوى الأمن المتطور:** في مستوى الأمن المتحكم فيه كل ما هو من المعقول تحقيقه بالوسائل والوقت المتاح تم فعله، ولتعريض نظام في هذا المستوى للخطر على المهاجم تصور هجمات معقدة، وهذا يتطلب خبرة حقيقية.

3.3.2 تفعيل طرق الحماية المناسبة

من أجل حماية أنظمة المعلومات، وحماية المعلومات الموجودة في البيئة الرقمية لابد من تفعيل منظومة حماية متكاملة تبدأ من الحماية المادية للموقع وقاعات المعلوماتية إلى الحماية البرمجية للأنظمة المعلوماتية، مع تكوين وتحسيس العمال بأهمية الموضوع وكيفية التعامل معه.

أ- **الحماية المادية**: وتتمثل في حماية موقع المنظمة وقاعات المعلوماتية عن طريق:

- **تقسيم المواقع الواجب حمايتها**: إذ يجب ترتيب المناطق الواجب حمايتها وتكييف معايير الحماية حسب حاجة كل منطقة، بوضع آليات الحماية وأنظمة الكشف بالداخل والخارج بين المستخدمين المسؤولين (Delbecque & Fayol, 2012, p. 95). ويكون هذا عن طريق مسؤول أمن أنظمة المعلومات ويكون لكل منطقة أمن خاص وشروط دخول محددة.

- **مراقبة الدخول للأنظمة**: الوصول المادي للتجهيزات يجب أن تكون ضمن سياسة مراقبة المداخل ومعرفة حاجات ومستويات السرية المسموح بها لكل مستخدم في المؤسسة لتجنب أي تشويه للمعلومات، سرقة الأجهزة أو تحاميل المعطيات (Carpentier, 2009, p. 39)، فالأجهزة المعلوماتية للمؤسسة يجب أن تكون محمية ضد كل دخول غير مسموح وبالتالي تكون الحماية المادية للأجهزة عن طريق إغلاق قاعات الخوادم والمعلوماتية والمكاتب وكل الأجهزة المتحركة التي تضم معلومات مهمة يمكن انتشالها.(Atelin, 2009, p. 32) وفي هذا السياق يمكن انشاء ما يسمى **بالغرفة التقنية** للموقع وهي عبارة عن مكان يحوي النظام العصبي المعلوماتي للمؤسسة والذي يجب أن يحظى بالحماية القصوى سواء من التدخلات البشرية أو من الكوارث الطبيعية.(Moinet, 2015, p. 137)

ب- **الحماية البرمجية**:

الحماية البرمجية تتمثل في استخدام كل البرامج المتاحة والتي توفر حماية للمعلومات المنتقلة عبر الشبكات أو المخزنة في الحواسيب، سواء عن طريق منع الدخول أو التشفير أو مكافحة الفيروس...، وتعتبر الحماية البرمجية أهم خطوة في تحقيق الأمن.

- **برامج مكافحة الفيروس**:

وضع برامج مكافحة الفيروس معيار أساسي في عملية الأمن، وهو برنامج ضروري ولكن غير كاف، لأن هذه البرامج لا تستطيع اكتشاف كل الفيروسات، من الضروري التيقن أنه ليس لمجرد عدم وجود أي اشعارات بإصابة الحاسب أنه سليم، لا يوجد شبكة سليمة 100% لأنه لا يوجد أي مكافح فيروسات يحمي 100% لذا بات لزاما على المؤسسات التفكير في منظومة حماية متكاملة وبرامج حماية مرافقة لهذا البرنامج لكي يعطي مفعوله.(Moinet, 2015, p. 12)

- **الجدران النارية**

فالجدار الناري يعمل على اختبار بطاقات تعريف كل مستعمل قبل الموافقة على دخوله الشبكة، فهو يراجع ويدقق الأسماء، عناوين بروتوكولات الانترنت (IP)، التطبيقات والخواص الأخرى لحركة المرور الداخلة، ويقارن هذه المعلومات مع قواعد الدخول التي برمجها مدير الشبكة في النظام، وهو يمنع كل الاتصالات غير المسموح لها التي تريد الدخول أو الخروج من الشبكة

سامحا للمنظمة بتطبيق سياسة أمن على حركة المرور التي تدور بين شبكتها وشبكات أخرى غير آمنة. (Laudon & Laudon, 2006, p. 372) ولكن من دون الاعداد الجيد للجدار الناري يصبح عديم الفائدة، وهناك طريقتين في إعداده:

- **السماح أولا**: مسموح لكل شيء المرور إلا ما تم منعه بشكل تخصيصي، وهي طريقة غير آمنة تجعل من الجدار الناري غير فعال.
- **المنع أولا**: كل شيء ممنوع مروره إلا ما تم السماح له بشكل تخصيصي، وهي الطريقة المثالية لتحقيق الأمن وجعل الجدار الناري فعالا.
- **الدخول المنطقي**:

تأمين الوصول المنطقي الخاص بمراقبة دخول المستخدمين لأنظمة المعلومات يرتكز على وسائل تقنية متطورة وعلى إجراءات استخدام هذه الوسائل التي تعرف وتحدد أدوار وحقوق كل مستخدم، حيث أن ترخيصات الوصول يجب أن تسير على أساس الوظائف وتطبيق مبدأ تحديد الصلاحيات والفصل بين الوظائف، وبفعل المناطق يجب تحديد من يستطيع الوصول وإلى أي مورد (Flaus, 2019, p. 295)

- **التشفير**

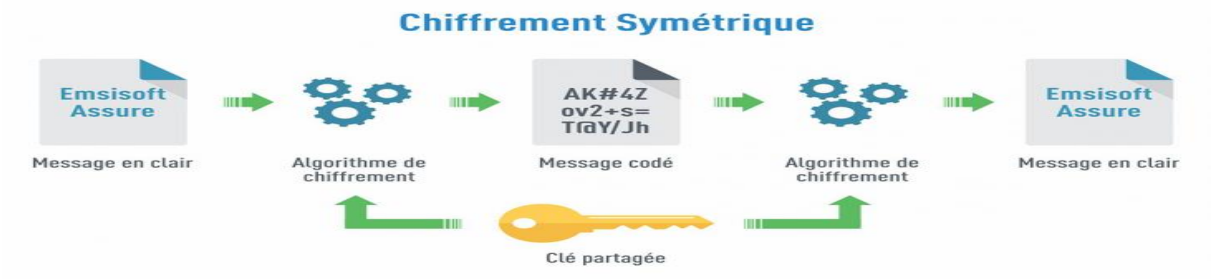
– "هو مجموع التقنيات التي تهدف إلى تحويل بفعل اتفاقيات سرية معلومات أو إشارات واضحة إلى معلومات أو إشارات غير واضحة من أجل تحقيق الفرضية المعاكسة عن طريق وسائل مادية أو برامج متخصصة لذلك". (Léopold & Lhoste, 2007, p. 72)

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

وهناك نوعين من التشفير (Flaus, 2019, p. 302)

– **التشفير المتماثل**: يكون مفتاح التشفير وفك التشفير هو نفسه ويجب أن يبقى سري خصوصا عند انتقاله بين المرسل والمستقبل.

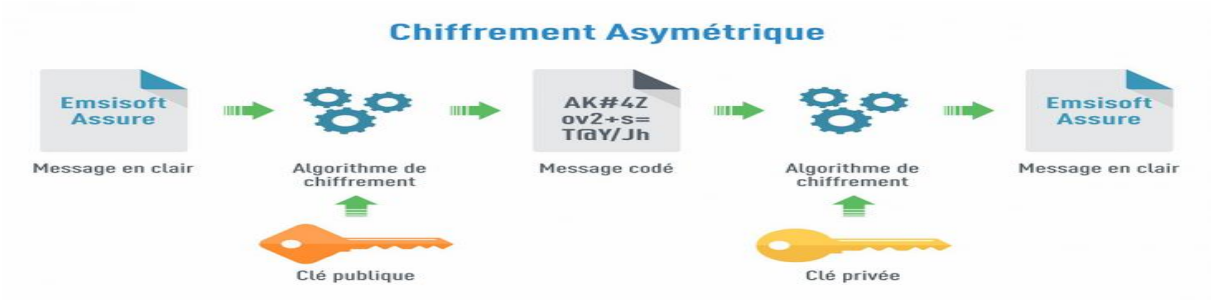
الشكل 2: التشفير المتماثل



Source: https://blog.emsisoft.com/fr/27699/rancongiciels-chiffrement/

- **التشفير غير المتماثل:** المفتاح المستعمل في التشفير مختلف عن المفتاح المستخدم في فك التشفير، وعليه يستلزم هذا النوع من التشفير مفتاحين: **مفتاح عام** للتشفير ويمكن إعطاءه للجميع، و**مفتاح خاص** يستخدم في فك التشفير، وهو شخصي ومعروف فقط من قبل مالكه.

الشكل3: التشفير غير المتماثل



Source: https://blog.emsisoft.com/fr/27699/rancongiciels-chiffrement/

- **أنظمة كشف التدخل**

– 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.

– أنظمة كشف التدخل تستطيع مراقبة نشاط الشبكة، مراقبة الحزم، تعريف امضاءات الهجمات الالكترونية المعروفة والتعديات من أجل إنذار الشخص المعني في حال اكتشاف مثل هذه النشاطات، فتكنولوجيا كشف التدخل تتيح للمنظمة معرفة صاحب التدخل وتكرار هجماته.

4.3.2 التكوين والتحسيس

على الرغم من ضرورة الحفاظ على سرية الترتيبات الأمنية، إلا أن العامل البشري يمثل الحلقة الأضعف في أمن المعلومة، ومن الضروري أن تتحقق لديه ثقافة أمنية تحسن من تصرفاته وترفع من قدراته في مجال أمن المعلومات، ولا يتم ذلك إلا برفع الوعي والتحسيس وتكثيف التكوين، والتحسيس ليس بالأمر الهيّن، إذ يعتبر تحدي لأغلب مسؤولي أمن أنظمة المعلومات، فالفرق الكلاسيكية يغيب فيها التأثير، ولا تحقق أهدافها بفعل اعتمادها المطلق على نشر الرسائل التي لا تصل ولا تؤدي مفعولها وسرعان ما تنسى، لذا ليس التحسيس عن طريق إلقاء المواعظ ونشر القواعد ما يحقق الفعالية، وإنما التحسيس بالتطبيق وإعطاء الأمثلة التي يفهمها المستخدم البسيط هو ما تحتاجه المؤسسة أما بالنسبة للتكوين ففي كثير من الأوقات المعلومة البسيطة التي يتم نشرها لا تكفي، ولمعالجة مواضيع حساسة ومعقدة من الضروري القيام بحصص تكوين حقيقية، وادماج هذه الحصص في إطار التكوين المستمر لإعطاء فائدة إضافية.

خاتمة البحث

الأمن المعلوماتي هو مفهوم شامل وعام يحمل تحت طياته العديد من أنواع الحماية نظرا لتعدد وتنوع الأجهزة والأدوات التي تحمل المعلومات، ولكن طريقة تطبيقه داخل المؤسسة هو أمر جد معقد، خصوصا مع ظهور النظريات الاقتصادية التي تنادي

بضرورة اشراك العمال في عمليات اتخاذ القرار واطلاعهم على كل نشاطات المؤسسة لتحقيق نتائج أفضل، فيحصل التضارب بين أن تتخذ المؤسسة سياسة مفتوحة واضحة المعالم وبين انتهاجها لسياسة متحفظة نوعا ما تحاول فيها حماية ارثها خصوصا المعلوماتي منه، وهنا تظهر فعالية المؤسسات في التحكم والتسيير الجيد دون التفريط أو الافراط في أي جانب من الجانبين،ومن خلال هذه الدراسة تم التوصل إلى **النتائج** التالية:

- تحقيق الأمن المعلوماتي على مستوى المؤسسات أمر ضروري في تحقيق أمن المعلومات وبالتالي تحقيق أمن المؤسسة، وعند تحقيق المؤسسات لأمنها المعلوماتي يتحقق بذلك الأمن الاقتصادي الذي يمثل الركيزة الأساسية للذكاء الاقتصادي والجانب الدفاعي له.
- زادت الحاجة للأمن المعلوماتي بتطور المعلوماتية وتعقدها وظهور تهديدات ومخاطر من نوع جديد يصعب التحكم فيها بالطرق التقليدية.
- الأمن المعلوماتي ليس مفهوم يطبق عن طريق تركيب أحدث الأنظمة والبرمجيات بل علم يتطلب إعداد استراتيجية متكاملة تغطي جميع الجوانب من تحقيق لأمن أنظمة المعلومات، وتحسيس وتكوين العمال لكيفية التعامل مع الأنظمة.
- التهديدات المعلوماتية دائمة التغير والتطور، وهذا يتطلب التطور المستمر والدائم لطرق وأساليب الحماية وعدم الاكتفاء بالوسائل الموجودة، فمثلا اعتماد مؤسسة ما على مضادات الفيروس أو الجدران النارية لحماية أنظمتها أصبح يعتبر في الوقت الراهن سذاجة من المؤسسة.
- تحقيق عنصر السرية الذي يعتبر أهم عناصر الأمن المعلوماتي في الوقت الذي يطالب فيه الجميع بالشفافية والوضوح، (إذ يرى كل فرد أو هيئة تتعامل مع المؤسسة أن لها الحق في الاطلاع)، هو معادلة جد صعبة تتطلب خبراء في الميدان، وهنا يتجلى دور العامل البشري وتظهر أهمية تكوينه وتدريبه.

التوصيات

- على المؤسسات العمل على تحقيق المعادلة الحساسة المتمثلة في بث المعلومة التي تعتبر مرحلة مهمة من مراحل الذكاء الاقتصادي مع الحفاظ في نفس الوقت على سرية المعلومة التي تعتبر أهم خاصية من خصائص الأمن المعلوماتي.
- على المؤسسات مهما كان نوعها أو حجمها أن تولي أهمية كبيرة للأمن المعلوماتي، وتطبيقه من خلال استراتيجية متكاملة تضم الأمن المادي والبرمجي مع إعطاء الأولوية للجانب البشري.
- تطبيق الأمن المعلوماتي يجب أن يكون في ظل رؤية استراتيجية واضحة المعالم تنطلق من تشخيص الوضع الحالي ومعرفة مستوى الأمن المطبق من أجل الوصول إلى الأهداف المرجوة.
- توفير مراكز لتعليم أساسيات أمن المعلومات والتدريب عليه بشكل عملي، والاهتمام بالبحث والتطوير في هذا المجال.

المقترحات

من خلال نتائج البحث نقدم بعض المقترحات للبحث فيها والتعمق أكثر في الموضوع:

- دراسة مدى أهمية وتأثير العامل البشري على مستوى أمن المعلومات في المؤسسة.

- دراسة حول أكثر وسائل الحماية استخداما من طرف المؤسسات العربية.
- دراسة مقارنة بين مستوى التطور المعلوماتي في المؤسسات العربية والغربية.

المراجع

المركز القومي للمعلومات. (2010). *مقدمة عن سياسات ومعايير أمن المعلومات*.السودان: المركز القومي للمعلومات–قسم الجودة والتطوير–.

الغثبر خالد بن سليمان ، و مهندس محمد بن عبد الله القحطاني. (2009). *أمن المعلومات بلغة ميسرة*.مكتبة الملك فهد الوطنية.

العزب، مأمون. (2018). *أمن المعلومات في فضاءات انترنت الأشياء. مجلة التقدم العلمي* (العدد 99).

ACISSI. (2009). *Sécurité informatique-Ethical Hacking*-.ENI.

Atelin, P. (2009). *Réseaux informatiques-notions fondamentales*-(3e ed).ENI.

Bloch, L., & Wolfhugel, C. (2009). *Sécurité informatique: principes et méthodes à l'usage des DSI, RSSI et administrateurs*(2eéd.).Eyrolles.

Bloch, L., & Wolfhugel, C. (2011). *Sécurité informatique: principes et méthodes*(3eed).Eyrolles.

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

Centre national de ressources et d'information sur l'intelligence économique et stratégique. (2014). *portail de l'IE*. IES. http://www.portail-ie.fr/lexiques/read/44

Delbecque, E., & Fayol, J.-R. (2012). *intelligence économique*.Vuibert.

Fernandez-Toro, A. (2016). *sécurité opérationnelle-conseil pratique pour sécuriser le systéme d'information* (2e ed). Eyrolles.

Flaus, J.-M. (2019). *Cybersécurité des systémes industriels*.ISTE.Ltd.

Fréminville, M. d. (2019). *la cybersécurité et les décideurs-sécurité des données et confiance numérique*-. ISTE.Ltd.

Gloaguen, P. (2014). *le guide de l'intelligence économique*.Hachette.

Godart, D. (2005). *sécurité informatique: risques, stratégies et solutions* (2eed).CCI de Wallonie s.a.

Guide N65. (2006). *Menaces sur les systémes informatique*.bureau conseil de la direction centrale de la sécurité des systémes d'information.

Lafitte, M. (2003). *Sécurité des systémes d'information et maitrise des risques*. Revue Banque.

Laudon, K., & Laudon, J. (2006). *Management des systémes d'information* (9ᵉed).Pearson.
Legendre, J. P. (2006). *"intelligence économique" guide pratique pour les PME*.MEDEF.
Léopold, E., & Lhoste, S. (2007). *la sécurité informatique* (3ᵉed). Puf.
Longeon, R., & Archimbaud, J.-l. (1999). *guide de la sécurité des systémes d'information à l'usage des directeurs*.Centre National de la Recherche Scientifique(CNRS).
Martre, H. (1994). *intelligence économique et stratégie des entreprises*.commissariat général au plan.
Matthieu Bennasar, A. C.(2007). *Manager la sécurité du SI-planifier, déployer, controler, améliorer-*. Dunod.
Moinet, N. (2015). *la boite à outils de la sécurité économique*.Dunod.
Pardini, G. (2009). *introduction à la sécurité économique*. Lavoisier.
Pelletier, A., & Cuenot, P. (2003). *intelligence économique-mode d'emploi-Maitrisez l'information stratégique de votre entreprise*.Pearson.
Philippe Clerc .(2013) .*la veille stratégique institutionnelle*. Association internationale francophone d'intelligence économique CCI.
Rouhier, S. (2008). *protection de l'information-enjeux,gouvernance et bonnes pratiques-*. Cigref.
Vaucamps, A. (2010). *Sécurité des routeurs et controles du trafic réseau*. ENI.

Seven issue - Part I July 2021 - Second Year Refereed Quarterly Scientific Journal

American International Journal of Humanities and Social Sciences

ISSUED BY AMERICAN INTERNATIONAL ACADEMY FOR HIGHER EDUCATION AND TRAINING

QUARTERLY JOURNAL ON HUMANITARIAN AND SOCIAL AFFAIRS

ISSN - 2710 - 4834

Deposit number in the Iraqi National Library and Archires: 2460