المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

الذكاء الاقتصادي ودوره في حماية الأملاك المعلوماتية

د. سليم برشيد عبد القادر
كلية الاعمال ـ جامعة الملك خالد – السعودية
البريد الالكتروني: smouali@kku.edu.sa

د. زياد العكروت
كلية الاعمال ـ جامعة الملك خالد – السعودية
البريد الالكتروني: zakrout@kku.edu.sa

الملخص

ارتبط كثيرا مفهوم الذكاء الاقتصادي بأنظمة المعلومات وحمايتها، وهو بذلك يشكل احدى الادوات المهمة في ادارة وحماية المعلومات في العالم الحديث، وذلك لما اصبحت تشكله عملية الحصول على المعلومات بطريقة غير شرعية من تهديدات امنية، اقتصادية وسياسية على سيادة واستقلالية الدول، ومن هنا فان وجود نظم حماية متطورة ترتكز على انظمة الذكاء الاقتصادي تشكل حاجز وقائي وحمائي يساهم بشكل او باخر في مواجهة التحديات الاقتصادية وحماية الاقتصاد الوطني، ومن هذا المنطلق سنحاول في هذه الورقة التطرق الى اهم العناصر المرتبطة بالذكاء الاقتصادي، انظمة حماية المعلومات، وكيفية مساهمة الذكاء الاقتصادي في حماية المعلومات.

الكلمات المفتاحية: النظام، الذكاء الاقتصادي، المعلومات، التنافسية.

تصنيف JEL: O53, O32, E61, D38

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

Economic Intelligence and its Role in Protecting Information Assets

Dr. Salim Bershid Abdel Qader
College of Business - King Khalid University - Saudi Arabia
Email: smouali@kku.edu.sa

Dr. Ziad Akrout
College of Business - King Khalid University - Saudi Arabia
Email: zakrout@kku.edu.sa

ABSTRACT

The concept of economic intelligence has been closely linked to information systems and their protection, and thus it constitutes one of the important tools in managing and protecting information in the modern world, because the process of obtaining information illegally has become security, economic and political threats to the sovereignty and independence of states, and hence the existence of systems Sophisticated protection based on economic intelligence systems that constitute a preventive and protective barrier that contributes in one way or another to facing economic challenges and protecting the national economy. From this point of view, we will try in this paper to address the most important elements associated with economic intelligence, information protection systems, and how economic intelligence contributes to protecting information.

Keywords: system, economic intelligence, information, competitiveness.

JEL rating: O53, O32, E61, D38

JEL Classification : D38, E61, O32, O53.

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والإجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

تمهيد:

لقد أدرجت العديد من التعاريف الخاصة بالذكاء الإقتصادي إلي أن السيطرة وحماية المعلومة الإستراتيجية بأنها إحدى عناصره[1] و تشير (Sophie Larivet) بأن للذكاء الإقتصادي وظيفة و تتمثل في إدارة المخاطر المعلوماتية[2] و ذكر (Philippe Clerc) وظيفة كشف التهديدات و التي تمثل إحدى الوظائف الثلاثة للذكاء الإقتصادي[3] ويجمع الباحثون بأن الذكاء الإقتصادي يتضمن الحماية من التهديدات والحماية الأمنية للمعلومات و أن الحماية تدخل في سياق الذكاء الإقتصادي الدفاعي و التي تخص حماية الإستراتيجية والمعارف والدراسات و الأملاك العلمية والتكنولوجية للمنظمة و مواجهة التهديد الذي يأتي من الدعايات الكاذبة الموجهة ضد المنتوج من حيث آثره على المستهلك والتي قد تنشر عادة في مواقع الأنترنت والذي عندما تتناوله الصحافة فإن الطلب عليه يتأثر في السوق . ومما سبق نري بأن الحماية في إطار الذكاء الاقتصادي تمس الجانب المعلوماتي الممتلك والحماية من حرب المعلومات.

أولا- الحماية المعلوماتية أو الأمن المعلوماتي

الأمن المعلوماتي والذي يجب أن يصمم لحماية المعلومة الحساسة بحيث يؤدي نشرها إلى التقليص من المزايا تنافسية وبالتالي مراعاة التهديدات والمخاطر. فالمخاطر تعني إمكانية حدوث حادث خارج عن الإرادة والذي قد يؤدي إلى فقدان الشيء أو الضرر به أما التهديد فقد يؤدي إلى أذى الآخرين أو أشيائهم ويقصد بالشيء أو أشيائهم المعلومة أو الوسائل المادية الخاصة بتخزين وإدارة المعلومة.

أمن المعلومات هو علم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها و ذلك من خلال توفير الأدوات و الوسائل لحماية المعلومات من المخاطر الداخلية أو الخارجية[4] و يعتبر أيضا أمن المعلومة مجموعة من الوسائل أو الإمكانيات النشطة و الدفاعية لضمان حماية التراث المعلوماتي للمنظمة و نشاطاتها". وتعرف الحماية المعلوماتية من الناحية:

- ✓ الأكاديمية: العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.
- ✓ التقنية: الوسائل والأدوات والإجراءات اللازمة توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.
- ✓ القانونية: التشريعات التي تهدف إلى حماية المعلومات من الأنشطة الغير مشروعة التي تستهدف المعلومات ونظمها[5].

تأخذ التهديدات عدة أشكال ومن بينها[1] الجوسسة وتخص كل التهديدات ذات الطابع الإستراتيجي و اختلال أنظمه المعلومات الآلي وقد تكون سببها إنتقاميا و سرقة المعطيات أو المصادر أو الغش المادي باستعمال معطيات

---

[1] حميدوش أمحمد، الذكاء الاقتصادي "فهمه وإنشاؤه وتأصيله و إستعماله"، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية و علوم التسيير، جامعة الجزائر 3، جانفي 2014، ص 278.

[2] Larivet Sophie, (2002), les réalités de l'intelligence économique en PME, thèse pour l'obtention de doctorat en Sciences de Gestion, Université de Toulon et du Var, 2002 (cité dans Ilhème Ghalamallah et les autres, Intelligence économique : proposition d'un outil dédié à l'analyse relationnelle, SciWatch Journal, Volume 3, Issue 2, 2008, p 6).

[3] Philippe CLERC, Encyclopaedia Universalis, 1995, p. 195.

[4] محمد بن سعود آل سعود، تدفق المعلومات بين الحرية والأمن في بيئة العمل الحكومية، مؤتمر تقنيات المعلومات والأمن الوطني، مجلة الاتصالات والعالم الرقمي، العدد 234، 2007، ص 535-536.

[5] موضي بنت عبد المحسن الخميس، دور مراكز المعلومات في دعم القرار السياسي، مؤتمر حول تقنية المعلومات والأمن القومي، الرياض، المملكة العربية السعودية، 1-4 ديسمبر 2007، ص 79.

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

منسية أو غير محدقة من طرف المنافسين وقد تكون ناجمة عن تهديد اللعب واللهو. فالتهديد التخريبي يعتبر الصنف الأقصى والهدام ويميز (François Jakobiak) بين صنفين من التهديدات[2] و هما:

✓ التهديدات والناجمة عن حوادث سواء عن كوارث طبيعية كالزلزال أو فيضانات أو حوادث مثل الحريق أو الناجمة عن الأخطاء المختلفة والغير مقصودة وترجع لقلة الخبرة أو الكفاءة أو خطأ في الإرسال أو حذف معلومات والتي يتم تقليصها عن طريق عمليات دورية تكوينية.

✓ التهديد العمدي الناجم عن عدة أغراض منها:

- تهديدات ذات طابع إستراتيجي وتهدف إلى الحصول على المعلومات الخاصة بأهداف وإدارة المنظمة لغرض اكتساب حصص جديدة في السوق ومعرفة التفاصيل الحديثة للأبحاث وطريقة الإنتاج الجديدة والإحاطة بأعمال التطوير لغرض التحدي.
- تهديدات ذات طابع إيديولوجي وتخص مجال الدولة وفي بعض القطاعات كالطاقة وصناعة الأسلحة مثلا.
- التهديدات المتعلقة باللعب بحيث يقوم بعض التقنيين الشباب محاولة اختراق العوائق الرقمية بإستعمال تقنيات لإظهار قدراتهم لرفع تحديات.
- التهديدات الجشعة والتي تفاقمت مع تطوير المعلومات الآلية والرقمنة والعمل على الشبكات وقد تأتي من داخل المنظمة أو من بين التهديدات الإلكترونية بحيث نجد:
  - تهديد TEMPEST كل نظام الإرسال الكتروني والذي يفوق أكثر من 100 متر يتم اكتشاف محتواه.
  - شفرات السيلكون .RFID[3] ترسل معطيات على مسافة بوسائل راديوا كهربائية وتسمى باللصيقة الذكية (étiquettes intelligence) تستعمل هذه التكنولوجية في إدارة المخزون والمحلات الكبيرة وبالتالي يمكن رصد المعطيات على مسافة إرسال وبالتالي تمكن من إعطاء معلومات حول تدفقات توزيع أحد الصناعيين مثلا.
- وأخيرا تهديدات الانتقام بحيث مثلا إجراء الطرد لأحد العمال بطريقة تعسفية يكون محور تهديد يصعب مواجهته.

أما فيما يخص المخاطر والتي تواجهها المعلومات والموجزة فيما يلي:

✓ الحوادث: وتخص مجموعة من المخاطر كانقطاع التيار الكهربائي وحالات الشغب وهذا كله يسبب فقدان المعلومات أو سرقتها أو التزوير فيها.

✓ مشاكل تقنية: وقد تتسبب في الفقد الكلي أو الجزئي للمعلومة أو حتى تسريبها.

✓ الجرائم الإلكترونية: تغلب على هذه الجرائم الخاصة بالحصول على المعلومات على الأجهزة والأشخاص أو الجهات بشكل مباشر أو بشكل غير مباشر.

✓ الإهمال: والذي يرتكز على العامل البشري المستخدم للأنظمة ومدى معرفته للتدابير الأمنية التي يجب عليه إتباعها ومدى حرصه على تطبيقها وأن أي إهمال أو تقصير في تطبيق تلك التدابير قد يسبب خطرا على المعلومة أو أمنها.

ومن خلال المقاربة النظامية للأمن approche Système وفق سياق الذكاء الاقتصادي في بعده الغائي téléologique يتم القيام بالتحليل الاستراتيجي للأمن من حيث الضعف والتهديدات والمخاطر risques وحتى النظر في الخطورة danger من مقاربة تخص علوم المخاطر les cindyniques.

الأمن المعلوماتي يفترض ضمان الأمن الإداري والمادي و الأمن علي نظام المعلومات أو التأمين علي نظام المعلومات[4] و الذي يعتبر جزء لا يتجزأ من الأمن الشامل الذي يهدف إلى الحماية من الهجومات:

---

[1] François Jakobiak, François Jakobiak, l'intelligence économique en pratique, comment bâtir son propre système d'intelligence économique, Éditions d'organisation, 2ème Edition, France, 2001, p 235.

[2] Ibid, p234.

[3] Pierre Lasborde, opcit, p 142.

[4] حميدوش أمحمد، مرجع سابق، ص 115 - 119.

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والإجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

✓ المادية: هذه الهجومات تسعي إلي التحطيم و تقصد المنشآت المادية لمنظومة المعلومة كالكابلات و أجهزة الكومبيوتر

✓ الإلكترونية وتخص التشويش على الاتصالات ووظيفتها وجعل نظام المعلومات غير قادر لتشغيل والاعتراض وتخص اعتراض الرسائل الإلكترونية القادمة من نظام معلومات ومن أهمها نظام (Echelon) الأمريكي الذي هو ناتجة الحرب العالمية الباردة ويستعمل 120 قمر صناعي لالتقاط ملايين من الرسائل في الدقيقة وتسيره الوكالة للأمن القومي (National Security Agency) وكذلك محطة الاستماع البريطانية (Menwith) في (Yorkshire)

✓ الواردة في البرمجيات والمتمثلة في:

- المسح: وتخص إرسال لنظام مجموعة معلومات مختلفة قصد التحديد بعد ما ينجم عن ذلك رد إيجابي.
- التفخيخ: إدخال وظائف مخفية من طرف المهاجم في نظام المعلومات
- البحث: دراسة منهجية للملفات في نظام لاستخراج معطيات هامة من طرف المهاجم.
- القناة المخفية: تمكن من استخراج عن طريق مختلف القنوات معلومات مخفية مفتاحية بالتعدي على سياسة الأمن ويهتم هذا النوع من الهجوم بأنظمة وقاعدة المعطيات عند مختلف مستويات السرية.
- التنكر: هجوم إعلام آلي يقدم نفسه بشخصية مختلفة لحصول لأعلى الحقوق من المفترض أن يتحصل عليه صاحب الامتياز.
- إعادة اللعب: وهو نوع من التنكر بحيث يرسل ولوج سبقه مستعمل وقام بتسجيله لدخول في نظام المعلومات.
- الإحلال: يكون الهجوم باعتراض طلب الخروج لمستعمل ويحل محله ويواصل العمل بدون أن يفطن النظام لتغيير المستعمل.
- الاندساس: المهاجم يكون في الشبكة على أساس انه هو مالك الحاسوب.
- التشبع: يتضمن ملأ منطقة التخزين أو قناة الاتصال إلى غاية الاستعمال.
- حصان طروادة: يتضمن وظيفة مخفية يعرفها المهاجم لوحده تمكنه من الالتفاف على المراقبة الأمنية السارية.
- السجق (salami) تمكن هذه التقنية من جلب معلومات جزئية من نظام معلومات وتراكمها بدون من أن يتم ملاحظة ذلك وتجميعها تدريجيا.
- الهائش (Trappe): نقطة دخول في تطبيق تسهيل ضبط البرامج وقد لا يتم التخلي عنها بعد بيع البرمجيات قد يمكن استعمالها للف عن إجراءات الأمن.
- القنبلة: برنامج طفيلي ينطلق في تاريخ معين وقد يكون خطير على نظام المعلومات.
- الفيروسات: هو برنامج قادر أن يتكاثر في نظام المعلومات ويسبب ضرر وفي بعض الأحيان تكون وخيمة.
- Ver: يجعل النظام في حالة عطل والهدف منه الحصول على معلومات عن طريق أسئلة عينة.
- الدودة: هو برنامج قادر على تحويل شبكة والتشويش عليها أو تعطيلها وهو نوع من الهجوم يستعمل بالاستيلاء على المعلومات عن طريق صبر الآراء للأنظمة.
- Asynchronisme المتزامنة: يستغل التوظيف المتزامن لدي البعض ثم إعادة استعمالها عند الطلب عليها وبالتالي يجد بالضرورة إطار للتسجيل والمهاجم يمكنه التغيير لتحايل على إجراءات الوظائف الأمنية.
- الباطني: هذه التقنية لا تهتم بالهجوم على نظام الأمن وإنما على عنصر الذي يدعمها مشغلا ضعف النظام.
- رموز السريات (cryptanalyse): تهتم بمعرفة أسرار الرموز لرسائل والذي عرفت اهتمام بتطور التجارة الإلكترونية.
- التصدير: وتخص خداع مستعمل الأنترنت كصفحة وهمية لموقع مصرفي أو تجارة إلكترونية للكشف عن معلومات سرية مثل الاسم واللقب والأرقام السرية ورقم Pin للإستعمالها.

يمكن تصنيف مختلف أنواع المهاجمين إلي نوعين وقد يكون من الداخل ليمارس التدليس مثلا مع توفر معرفة جيدة للإعلام الآلي كالرغبة في الانتقام لعدة أسباب و النوع الثاني من الخارج و قد يكون له عدة دوافع كالغش لغرض تحويل أموال و القرصنة و الهاكر (hacker) و يسمون بالقبعة الرمادية عندما يكون هجومهم مبني على أساس اللعب أو رفع تحدي ويحملون تسمية هاكر ذات القبعة السوداء الذين ينشرون الفيروسات لغرض الجوسسة والقرصنة أما الهاكر ذات القبعة البيضاء الذين يدخلون مع احترام القانون و يتعاكس الهاكر مع الكراكر(crackers) لأن هذا الأخير يسعي إلي الاقتحام فقط إ بكل الوسائل المتاحة لديه. ومع تطور وإستعمال

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

وسائل تكنولوجيات الإعلام والإتصال تتنوع أشكال الهجوم من الخارج مثل الكراشر والمختص في الهجوم على نظم البطاقات التي تحمل شفرات السيلكون و (Phreaker) الصنف الجديد من القراصنة والمختص في الولوج عبر شبكات الهواتف.

كما أن هناك البريد الذي يسبب إزعاج ولا يسبب على العموم أضرار ويخص كل من:

- ✓ SPASM أي بريد إلكتروني يرسل بطريقة ألية وهو غير مرغوب فيه و يتسبب في تشبع البريد الإلكتروني و قد أشارت مجموعة فرنسية بأنها تتبادل 500 ألف رسالة إلكترونية يوميا و ترمي 60 ألف بحيث 51% منها تمثل SPASM والباقي فيروسات ويعتبر عدو ليس لخطورته ولكن للإزعاجات و الإرهاصات[1].
- ✓ Spyware رمز يمكن من إرسال عادات سلوك مستعمل الأنترنت و الذي يمكن إعتباره برمجية جوسسة و لكن مع أهداف تجارية أو للقيام بالدراسات هدفها التسويق ..الخ كما يمكن من أن يحتوي على برامج ضارة والتي تؤثر على سرية المعطيات للمستعمل الأنترنت[2].
- ✓ adware : برامج تمول عن طريق الإشهار ويرجع بصفة ألية الإشهار ، وقد تكون على شكل Popup أي أشكال من الإشهار على خط www الموجهة لجلب حركة على الأنترنت وجلب عناوين بريد الكتروني وتستعمل في واجهة أو على الشاشة خلال تنصيب البرنامج[3] والفرص لتحقيق عائد لصاحبه و في الأصل غير ضارة و بعضها يدمج أو يحمل برامج جاسوسية.

كما أن الهجومات المعلوماتية قد تخص كل من:

- ✓ العنصر البشري: الفرد هو العنصر الأساسي في نظام المعلومة ويشكل الهدف المفضل وقد يكون محل تلاعب بأهداف لاستخراج منه المعلومة.
- ✓ المجال التنظيمي: استعمال عيوب التنظيم والمكان للوصول إلى مصادر حساسة.

الأهداف الرئيسية للهجوم حسب (Pierre LASBORDE) تشمل عموما خمسة جوانب[4] وهي:

- ✓ التضليل الإعلامي
- ✓ منع الولوج إلى مصدر على نظام المعلومات،
- ✓ السيطرة على النظام لاستعماله لا حقا،
- ✓ جلب المعلومة الموجودة على النظام،
- ✓ استعمال النظام للقفز إلى نظام قريب له.

يعرف (Audrey KNAUF) الأمن بالعملية التي تهدف الحماية من المتسللين الخارجيين أو من فقدان المعطيات لا سيما من خلال التأمين على نظام المعلومات[5]. و تتطلب عملية التأمين حسب (Fabrice) كل من [6]:
[6].

[1] Pierre LASBORDE, la sécurité des systèmes d'information: un enjeu majeur pour la France, rapport du 26 novembre 2005, la documentation Française, p 30.
[2] IBID.
[3] en.wikipedia .org/ wibi/Adware (visité le 12/02/2014).
[4] Pierre LASBORDE, opcit, p 20.
[5] Audrey KNAUF, caractérisation des rôles du coordinateur animateur : émergence d'un acteur nécessaire à la mise en pratique d'un dispositif régional d'intelligence économique, thèse de doctorat en sciences de l'information et de la communication, Université de Nancy 2, École doctorale langages, temps, Sociétés, France, 2007, p 48.
[6] Fabrice Frank, fondement d'une politique de sécurité globale des systèmes d'information au au sein d'une grande entreprise, communication sur la gestion des risques, thèse de master en management des systèmes d'information et des technologies , École des Mines de Paris France, 2002, p 37.

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

- ✓ الإدراك بوجود مخاطر.
- ✓ تحديد الذي لديه قيمة من خلال التصنيف.
- ✓ الترتيب بالنسبة لرهانات الأعمال.
- ✓ تشخيص الضعف: تدقيق، خبرة – دراسة.. الخ.
- ✓ حذف الازدواجية والضعف الكبير ومعرفة الرهانات الكبيرة بواسطة تقنية إدارة المخاطر.
- ✓ أخذ تدابير الحماية إذا وقعت حادثة: التخزين وعدم التساهل مع الإعطاب ووضع مخططات النجدة.
- ✓ أخذ إجراءات وقاية لتقليل من إحتمال وقوع أحداث: برامج مضادة للفيروسات وجرد الدخول والولوج.. الخ

سياسة مراقبة الولوج المنطقية تتمثل في ميكانزيم و الذي بموجبة يسمح أو يمنع النظام للأعمال المطلوبة من طرف فاعلين (الهيئات النشطة) على مواد objects (هيئات خاملة)[1] وبالتالي سياسة مراقبة الولوج المنطقية تعتبر من بين الإجراءات التي تمكن من ضمان أمن أنظمة المعلومات. هيكلة الحقوق هو التعبير عن لماذا وكيف مستعمل كيف يتحصل على الامتيازات وهيكلة الحقوق هو موضوع للنماذج الدخول أي الولوج[2].

مبدأ أدني المزايا هو مبدأ الأمن الذي يفرض على الفاعلين لأنظمة من أن تتصرف بأدنى مزايا التراخيص اللازمة لإنجاز المهام الموكلة لها[3] و الجدول التالي يبين مكان مراقبة الولوج في سياسة الأمن .

جدول رقم 1: تخصصات سياسات الأمن

نوع	وصف	أمثلة
مادي	تقييد الدخول المادي إلى الموارد	حواجز و خزائن (Coffre)مفاتيح ..الخ
إداري	تنظيم وإجراءات لتعزيز الأمن	تحقيقات ، تدقيق تمكين مسؤولية الممارسة الجيدة
منطقي	تقييد الدخول المنطقي إلى أجهزة الإعلام الآلي تديرها برمجيات ومعدات	التصديق، التحقق ، التشفير ، الفصل تنظيم الحقوق

Source: Romnald Thion, opcit, p 15.

أمن المعلومة سيرورة تهدف إلى صياغة المعطيات، وتطبق على كل جوانب الأمان والضمان والحماية للمعطية أو للمعلومة مهما كان شكلها و تنظيم أمن المعلومات يتطلب وضع سياسة الأمن وإجراءات التدقيق تمكن من التأكد من الفعالية .السياسة الأمنية تمثل مجموعة من نماذج التنظيم والإجراءات أحسن ممارسات تقنية تمكن من ضمان أمان sureté وأمن sécurité نظام المعلومات وتعرف سياسة الأمن أيضا بأنها مجموعة القوانين و القواعد و الممارسات التي تنظم الطريقة التي يتم بها إدارة المعلومة الحساسة والمصادر الأخرى وحمايتها وتوزيعها في النظام[4].

[1] Butler W lampson, protection ACM SIGOPS operating systems Review vol 8, issue 1, p 18-24, ACM Press, New York, 1994.

[2] Romuald Thion, structuration rationnelle des politiques de contrôle d'accès : représentation, raisonnement et vérification logique, thèse de doctorat en informatique, Institut des Sciences Appliquées de Lyon, École doctorale : informatique et information pour la Société, France, 2008, p 16.

3 M. J. Nash & K. R. Poland, some conundrums concerning separation of duty, IEEE Symposium on Security and Privacy, pages 201-209, 1990 (cité dans Romuald Thion, opcit, p 45).

[4] ITSEC , Information Technology Security Evaluation Criteria, V 12, 136 p, office des Publications officielles des Communautés Européennes, Luxembourg, 1991 (cité dans Anas Abou El Kalam, Anas Abou El Kalam, patrons organisationnels et techniques pour la

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والإجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

تنفيذ السياسة الأمنية على المستوى العملي يرتكز على بعض الوظائف كالتحديد والتصديق للهيئات ومراقبة الولوج وتعقب traçabilité المواضيع والعمليات، تدقيق الأنظمة، حماية المحتويات والإدارة للأمن هذه الوظائف هي بجد ذاتها محل تهديدات خاصة بها ويمكن أن تمثل نقاط ضعف تكون مجال للهجوم قد يكون له دوافع أم لا. و عند معالجة أمن المعلومة الإهتمام بها على أثرها مركبة من ثلاثة خصوصيات التوفر (disponibilité) و السلامة / النزاهة (intégrité) والسرية (Confidentialité) و التصديق(authentification) وعدم التنصل/ تنكر (non répudiation) و المحسوبية (imputabilité)[1].

إن من أدوات الحماية للمعلومات نشير إلي تحليل المخاطرة و التي يعرفها كل من (Nastovsk)[2] و (Hoffman) [3] بأنه مقياس تحليلي موجه لإرساء سياسة الأمن مع أخذ بعين الإعتبار نسبة تكلفة ربح في محيط حقيقي ومعقد وتتكون من :

✓ تقييم المخاطر وتتضمن تحديد المخاطر الموجودة ضمن نظام ونتائجها وتقييم فعاليات العروض والإجراءات المضادة المشتركة.

✓ إدارة المخاطر وتتضمن اختيار العروض التي تقلل من التعرض للمخاطر مع اخذ بعين الإعتبار العوائق الوظيفية وكذلك العوائق العملية ذات طابع الاجتماعي والسياسي ومالي

أما تشخيص المخاطر فيتطلب تدقيق الأمن الذي يمكن من تطبيق سياسة الأمن وتحديثها أو التوصل إلى خريطة نقاط الضعف ويتم القيام بالتشخيص حسب منظورين: و هما المنظور التنظيمي ويشمل تحليل جانب الأمن ومراقبة تطبيق إجراءات الأمن والتدقيق المادي للمقرات و المنظور التقني ويتضمن المعاينة التقنية وكشوفات التصاميم وتحليل رموز مصادر التطبيقات و إختيار تجريبي [4] .

فمن الجانب التنظيمي فقط يمكن اللجوء إلى عدة طرق المستعملة كالقياس رقم ISO 17799 الأكثر إستعمالا على المستوى الدولي. القياس ISO 17799 يعطي توصيات للإدارة الأمن المعلوماتي التي تم إنشاؤها لتطوير معيار لإدراج الثقة في العلاقات. هذه الطرق والمعايير تهيكل الإجراء لتقليص التجربة في قيادة سياسة أمن نظام المعلومات. نظام ISOيقسم أمن المعلومات الآلي إلى مجالات:

✓ التصديق ومراقبة الولوج: إن التصديق والتأكيد من مستعمل يكون سري يعرفه إلى وحده (رقم استعمال وسر المرور) بواسطة عنصر مادي الذي بحوزته سواء بطاقة مغناطيسية أو علامة مميزة أو خصوصية بيولوجية كالصوت والبصمات. في بعض الأحيان التصديق على المستعمل يرافقه التعريف على الحاسوب الذي ينظم إلى النظام.

✓ سرية معطيات الترقيم) chiffrement): الترقيم يمكن من تحويل نص مقروء إلى نص غير مستعمل (إذا لا نعرف طريقة التحويل المطبقة أو مفتاح الترقيم).

✓ استقامة المعطيات وعدم الإنكار حتى يمنع تزوير معطيات بواسطة وظيفة الشطر في إتجاه واحد ويمكن من حساب بصمة رسالة المرسل إليه بإعادة حساب البصمة فإن لم يجدها فهذا يعني بأن الرسالة تغيرت.

---

sécurisation des organisations virtuelles, thèse de doctorat en informatique, Université de Toulouse III, Paul Sabatier, France, 2008, p 14) .

[1] حميدوش أمحمد، مرجع سابق، ص 99و100.

[2] L.J Hoffman, smoking the bada chers : risk analysis in the age of micro–computer, Computer and Security, vol 8, p 299-302, 1989 (cité dans Elie BURSZTEIN, anticipation games, théorie des jeux appliqués à la sécurité des réseaux , thèse de doctorat en informatique, École Supérieure de Cachan France, 208, p 10.

[3] Z A nastovski, risk analysis in computer network, a review, technical report, Center for computer security research, Wollongong NSW, Australia, 1993 (cité dans Elie BURSZTEIN, opcit, p 10).

[4] Fabrice Frank, fondement d'une politique de sécurité globale des systèmes d'information au sein d'une grande entreprise : communication sur la gestion des risques, thèse de master en management des systèmes d'information et des technologies, École des Mines de Paris France, 20025, p 32.

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والإجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

✓ التصديق مثلا على إمضاء إلكتروني يوافق بين الشطر(hachage) في تجاه واحد والترميز السري ذا المفتاح العمومي وعدم الإنكار يمنع للمرسل إليه عدم إستقبال معلومة وتتم عن طريق تقاطع بين إمضاء الكتروني والتأثير المؤقت.

كما أن هناك طرق أخري تنظيمية تمكن من تحليل المخاطر ونشير إلي كل من طريقة:

- MARION[1] و تمكن من تقييم المستوى الأمني للمعلوماتية في منظمة من خلال إستبيان (عبارة عن طريقة التحليل وتقلص المخاطرة في المعلومات الآلية) و طور كل من النادي للإعلام الآلي الفرنسي و ASPAD منذ 1984 هذا النظام للتأمين علي نظام المعلومات الآلي في المنظمة. وتقترح هذه الطريقة الإجابة عن التساؤلات التالية: ما هي المخاطرة التي قد تتعرض لها المنظمة؟ وهل يمكن قبول هذه المخاطرة؟ وما هي قدرات المنظمة لتحمل الخسائر الناجمة عن هذه المخاطرة؟ وماهي العوائق؟ وكيف يمكن تحسين الأمن؟ وما هو المخطط الذي يجب وضعه؟ وتقترح الطريقة ستة مراحل وتتمثل في تحليل المخاطر (تحديد دقيق للمخاطر مع تحسيس الإدارة المسيرة) والحد الأقصى المقبول للمخاطرة وتحليل الوسائل من وجهة نظر أمنية (التدقيق والجرد للوسائل الخاصة بالأمن) وتقييم العوائق وإختيار الوسائل الأمنية. التوجيهات وكتابة المشروع يحتوي على ملخص يتضمن التقنية المنتظرة والميزانية والمخطط. تستعمل هذه الطريقة 27 مؤشر وترتب على ستة مواضيع كل مؤشر يعطي له نقطة 0 في حالة عدم الأمن و4 لما تكون الوضعية جديدة و3 آمن مقبول. هذه الطريقة تشمل الأمن التنظيمي والأمن المادي الذي هو إستمرارية التنظيم في الإعلام الآلي والأمن المنطقي وأمن التطبيقات وتمر الطريقة على أربعة مراحل:

- التحضر: تخص تحديد أهداف الأمن التي يجب بلوغها وكذلك مجال عمل التدقيق والتقسيم للنظام المعلومات التي يجب المصادقة عليه لتبسيط إنجاز الدراسة.
- دراسة الضعف وتخص الإستجابة عن التساؤلات وتمكن من جرد مخاطر نظام المعلومات والعوائق وعلى إثرها يتم رسم المبني على التقسيم لكل مؤشر وعوامل المخاطرة لرؤية نقاط الضعف التي يجب حمايتها.
- تحليل المخاطر وتمكن من ترتيب المخاطر حسب معيار التصنيف مخاطرة بالغة وبسيطة. التحليل يخص التهديدات وأثارها وإحتمالها وبالنسبة لطريقة يوجد 17 تهديد مثل حادث مادي، نسبة الضرر المادية والنقص عند المستخدمين، نقص الخدمات، عطل في نظام المعلومة، إنقطاع في سير الشبكة، خاصية في الكتابة، الخطأ في الإرسال، خطأ في الاستعمال وخلل في التصميم، تحويل أموال، اختلاس معدات، آلات مخفية لبرمجة، نسخ غير قانوني لبرمجيات، عدم التحفظ في تحويل المعلومة، التخريب والهجوم منطقي على الشبكة.
- مخطط عمل: يحاول من رفع 27 مؤشر إلى قيمة 3 مستوى أي أمن مقبول. ولقد تم التخلي عنها لصالح طريقة MEHARI.

✓ طريقة MEHARI[2] و هي طريقة منسجمة للتحليل مخاطر المعلومات الآلية و هي طريقة مبنية إنطلاقا من طريقة MARIO و تقوم علي أساس التقييم الحقيقي للمخاطر و مراقبة و إدارة الأمن المعلوماتي على المدى القصير والمتوسط والطويل مهما كان التوزيع الجغرافي للنظام المعلومات الآلي بحيث ترتكز علي :

- الإسداء أو الاستنتاج المنطقي (raisonnement) من العام إلى الخاص مع لا مركزية القرار في التسيير العملي للأمن.
- إعتبار الأمن من زاويتين: حماية قصوى للمخاطر وتماسك كل هياكل إزاء الأمن.

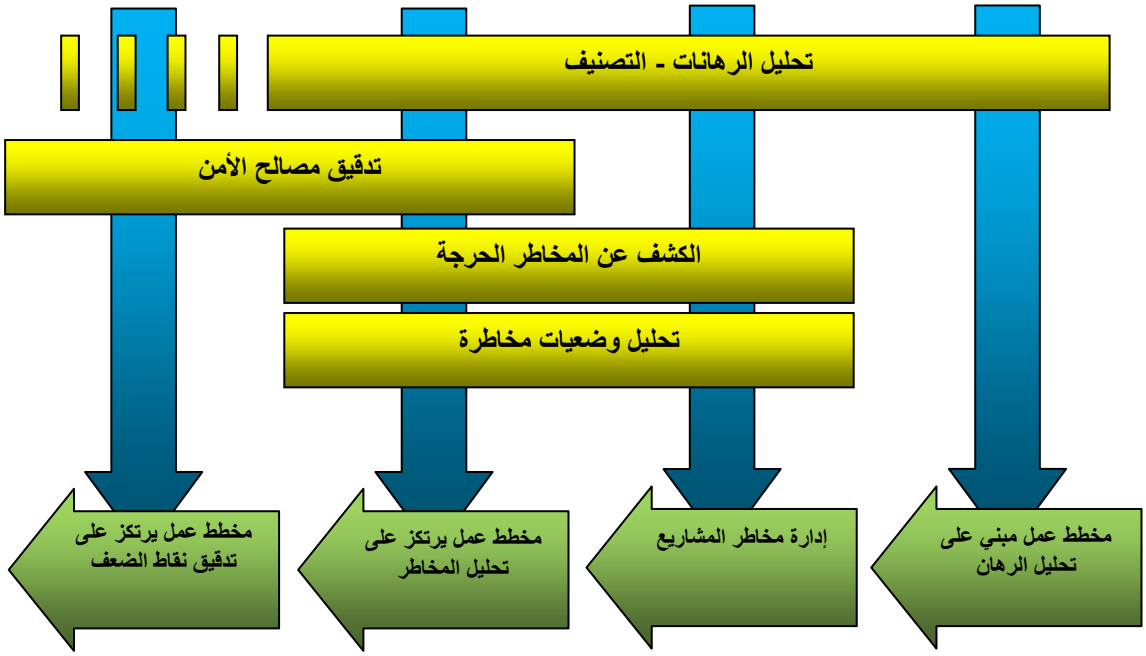
الارتكاز على السيطرة على المخاطرة والتي تكون الأكثر شفافية ممكن حتى يكون المستعمل لهذه الطريقة حر في اختياراته للاستراتيجية المناسبة. لقد طورت هذه الطريقة الجمعية الفرنسية لمستعملي الإعلام الألي و تخص تحليل رهانات الأمن من خلال تساؤل حول سيناريوهات الممكنة; و التي تتضمن الرهانات و التي تعبر عن خلل الذي يكون له أثر ضار ثم التدقيق لتحديد نقاط ضعف نظام المعلومة وأخيرا القيام بتحليل المخاطر والتي نوضحها في الرسم التالي:

[1] Méthodologie d'Analyse de Réduction de Risques Informatiques orientée par niveau
[2] Méthode Harmonisée d'Analyse de Risques.

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والإجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

شكل رقم 1: طريقة MEHARI



وتتمحور طريقة MEHARI حول ثلاثة مخططات وهي:

- المخطط الإستراتيجي للأمن والذي يحدد أهداف الأمن والقياسات التي تمكن من تقييمها وفي هذه المرحلة يتم تقييم مستوى خطورة المخاطر وتحدد سياسة الأمن وقواعد إستعمال نظام المعلومات من طرق المستعملين.
- المخططات العملية للأمن التي تحدد كل موقع إجراءات الأمن التي يجب أن تنفذ ولهذا تحدد سيناريوهات التساهل والتدقيق لخدمات نظام المعلومات. وعلى أساس هذا التدقيق يتم تقييم كل المخاطرة المحتملة والآثار التي تمكن من بعد تحديد حاجيات الأمن وكذلك إجراءات الحمايات اللازمة وفي الأخير التخطيط لتأهيل أمن نظام المعلومات.
- المخطط العملي والذي يضمن متابعة الأمن من خلال إعداد مؤشرات حول المخاطر وإختيار سيناريوهات الحوادث التي يجب الاحتياط لها.

طريقة MEHARI تقترح مسعى مركز على حاجية الاستمرار ليقدم دليل منهجي. فالتدقيق التي تقترحه هذه الطريقة تمكن من إنشاء مخطط عملي ملموس وتمكن من بناء سياسة أمن الموجهة إلى تغطية الضعف الملاحظ من خلال التدقيق والوصول إلى مستوى الأمن الذي يناسب أهداف التي حددها المخطط الاستراتيجي للأمن.

الهدف الرئيسي لطرق تحليل المخاطر هو أن يكون لدينا مفهوم عام متجانس لتطوير المستوى العام للأمن وتقدير بطريقة دقيقة للمخاطرة وتقدير وتحديد الأوليات من أهم الطرق بالإضافة إلى ما سبق نوجز طرق أخرى من أهمها[1] طريقة (MELISA)[2] و طريقة CRAMM[3] و هي شبيه لطريقة (MELISA) بحيث طورتها

[1] Daniel CREVOISIER, la sécurité et la qualité dans un système d'information hospitalier, Presse Polytechniques et Universitaires Romandes, sécurité et qualité informatiques « nouvelles orientations », contribution publiées sous la direction de Jean MENTHONNEX, Université Romandes, Lausanne, Suisse, 1995, p 360.

[2]Méthode d'Évaluation de la vulnérabilité résiduelle des systèmes d'informations

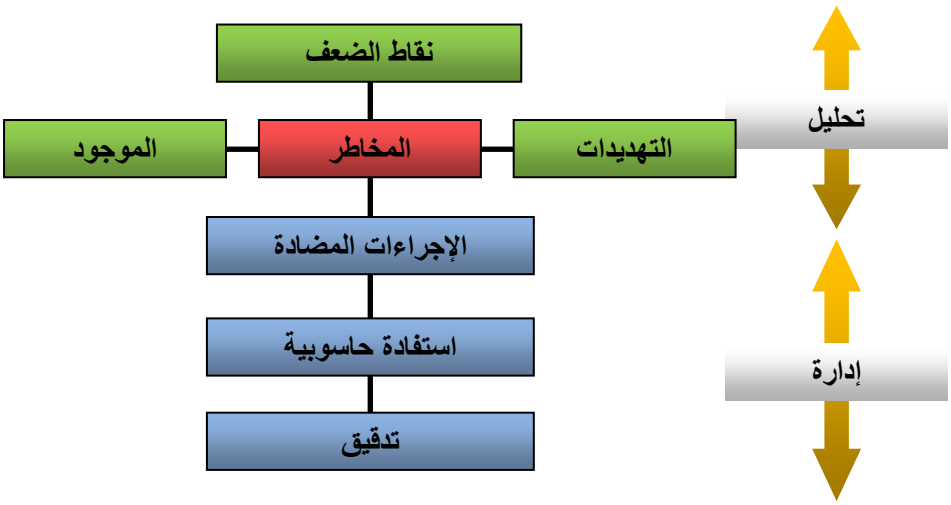
[3]central computer and telecommunication Agency- ACTC- Risk Analysis and Management Methodology

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

الحكومة البريطانية في سنة 1985 و التي تقوم علي معالجة الوسائل والتهديدات الناجمة من مجموعات مصالح مع إستعمال احتمالات تم تحديد (porades). هذه الطريقة ثقيلة تخص المنظمات الكبيرة لأها تهتم بي 3000 نقطة مراقبة وتحتوي على متغيرين إحداهما متناسق مع قياس الأمن BS 7799. الإجراء الخاص بطريقة CRAMM يظهره الرسم التالي:

شكل رقم 2 : الإجراء العام لطريقة CRAMM



وتتضمن طريقة CRAMM ثلاثة مراحل وهي:

- تحديد المتواجد (existant) من حيث جرد التجهيزات والتطبيقات والمعطيات التي تشكل هياكل الإعلام الآلي التي يرتكز عليها نظام المعلومات. كل عنصر لهذا الجرد يتم تقيمه من حيث التكلفة والأثار في حالة التساهل وعدم وجود والإتلاف والتحطيم.. إلخ.
- تقييم التهديدات والضعف مع إبراز المشاكل الممكنة ولهذا قاعدة المعرفة لي Gramm هو توفير قائمة هامة للمخاطر الممكنة التي يجب تقييم المستوى الحرج.
- إختيار العلاج: وتخص إختيار من بين قاعدة لي 3000 إجراء مضاد ممكن مصنفة على 70 موضوع مع العلاج الممكن للمخاطر التي تم تحديدها في المرحلة السابقة بواسطة مساعدة تقدمها برمجية.

- طريقة OCTAVE[1] و OCTAVE S في البداية كانت موجهة لمنظمات الكبيرة وحاليا توجد نسخة خاصة بالمنظمات الصغيرة. وتهدف هذه الطريقة إلى تمكين المنظمة من إنجاز تحليل للمخاطر الخاصة بنظام المعلومات وبدون اللجوء إلى خبرة خارجية وتقترح هذه الطريقة ثلاثة مراحل:

- النظرية التنظيمية: تبدأ بتحديد الأصول المادية والتهديدات التي تؤثر على السير الحسن وتحديد نقاط ضعف التنظيم وأهداف الأمن المفروضة من طرف المديرية وإجراءات الأمن الحالية وجمع المعلومات. سيرورات المعلومات تخص ثلاثة مجموعات وهي الإطارات العليا والإطارات العملية وفرق الإنتاج. ثم توطيد المعلومات من هذه السيرورات والتي تؤدي إلى إعطاء صور عن التهديدات.
- النظرية التقنية: تحديد العناصر الأساسية لكل أصل ثم تحديده في المرحلة السابقة والتدقيق لمعرفة نقاط الضعف.
- تطوير إستراتجية الأمن والتي تتضمن تقييم المخاطر التي تم تحديدها وآثار واحتمال الوارد وإقتراح إجراءات لتقليصها ومخطط تقليص المخاطرة الذي يتم التخطيط له.

[1] Operationally Critical Threat , asset and Vulnerability Evaluation

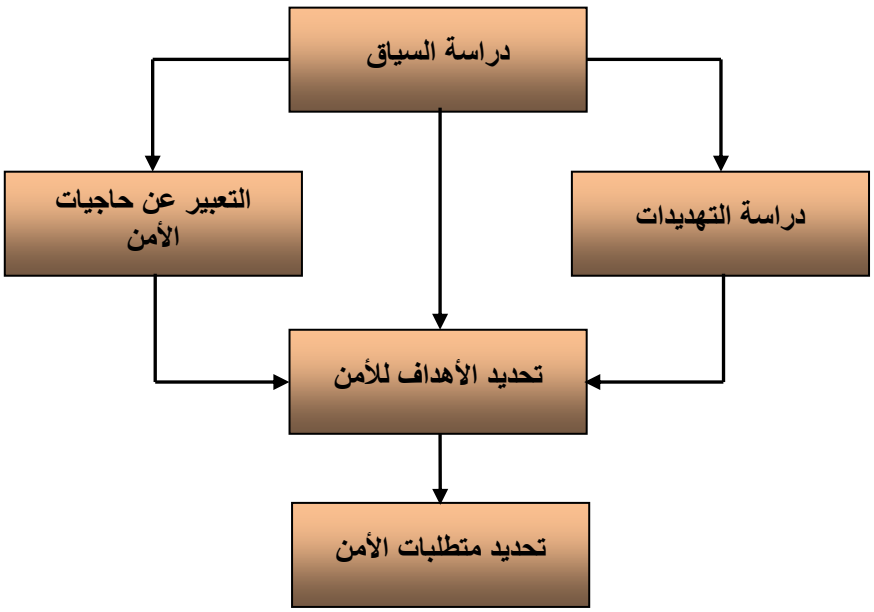
DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

هذه الطريقة ترتكز على حماية أصول المنظمة وإدارة المستخدمين وتغطية كل سيرورات المهن على كل المستويات التنظيمية والتقنية. وتفترض هذه الطريقة إنشاء فرقة متعددة الاختصاصات والمتضمنة أعضاء من مختلف المصالح بحيث تمكن من تحسين معارفهم وتعاضد الممارسات الحسنة للأمن.

✓ طريقة EBIOS[1] و هي تتميز بتحديد مخاطر نظام المعلومة وتقترح سياسة الأمن المكيف مع حاجيات المنظمة أو الإدارة . تتكون طريقة من 5 دلائل: المدخل، إجراء، تقنيات وأدوات وبرمجية التي تمكن من تبسيط المنهجية لهذه الدلائل. تشمل هذه الطريقة خمسة مراحل والموضحة في الشكل التالي:

شكل رقم 3: طريقة E BIOS الشاملة



Source : Michel Kamel[2]

هذه المراحل الواردة في الرسم نشرحها فيما يالي:

- دراسة السياق والتي تمكن من تحديد أي نظام المعلومات محل دراسة وتحدد أيضا محيط الدراسة: تقديم المنظمة، البنية الهندسية لنظام المعلومات، العوائق التقنية والتنظيمية، الرهانات التجارية. كما تدرس التفاصيل الخاصة بالتجهيزات والبرمجيات والتنظيم البشري.
- التعبير عن الحاجيات تمكن من تقييم المخاطر وتحديد مواصفات المخاطرة. مستعملين نظام المعلومة يعبرون في هذه المرحلة عن حاجيات الأمن حسب الأثار الذين يقيمونه بأنه غير مقبول.
- دراسة التهديدات: التي تمكن من تحديد المخاطر ليس حسب حاجيات المستعملين ولكن حسب البنية الهندسية لنظام المعلومة وبالتالي قائمة نقاط الضعف وأنواع الهجوم يتم إعدادها حسب المعدات وهندسة الشبكة والبرمجيات المستعملة وهذا مهما كان مصدرها: بشري، معدات، المحيط وأسباب حدوثها المعتمدة.

[1] Expression des Besoins et Identification des Objectifs de sécurité
[2] Michel Kamel, Patrons organisationnels et techniques pour la sécurisation des organisations virtuelles, thèse de doctorat en informatique, université de Toulouse (France), 2008, p 80.

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

- تحديد أهداف الأمن: توطد حاجيات الأمن المعبر عنها والتهديدات المحددة لإبراز المخاطر التي يجب أن يحمي منها نظام المعلومات. هذه الأهداف تكون محل دفتر الأعباء للأمن الذي يترجم الخيارات الخاصة بمقاومة التهديدات حسب متطلبات الأمن.
- تحديد متطلبات الأمن تمكن من تحديد إلى مدى ما يتم الوصول إليه في مجال متطلبات الأمن. فمن البديهي من تحديد كل أصناف المخاطر بعضها يتم قبولها حتى لا تكون التكلفة عالية وبعضها يقلص والبعض الأخر يرفض في إطار مخطط المخاطرة. يتم القبول حسب التكلفة الناجمة عن المخاطرة وإحتمال ونوعها لتبرير هذه المتطلبات يعطي ضمان لتقسيم عادل.

طريقة EBIOS تمكن من بناء سياسة الأمن حسب التحليل للمخاطر الذي يرتكز على سياق المستعمل لها والوضع المرتبط بنظام المعلومات.

✓ طريقة Cobit Control [1] و هي طريقة للمسيرين اللذين يرغبون في تقييم المخاطر (أمن و المصداقية و المطابقة) و مراقبة الاستثمارات في مجال تكنولوجيات الإعلام و الإتصال. هذه الطريقة موجهة لسيرورة بحيث كل نظام المعلومات وتتجزأ إلى 34 سيرورة مجمعة على 4 مجالات. أما الإطار التصميمي لهذه الطريقة يتمحور حول ثلاثة محاور وهي سيرورات تكنولوجيات الإعلام والإتصال ومواصفات المعلومة وموارد تكنولوجيات الإعلام والإتصال.

✓ CMMI[2] و هي طريقة تحسين سيرورات التي تقدم العناصر الأساسية لسيرورات الفعالة. و تقوم هذه الطريقة علي تقييم مستوى نضج المستعمل لها في مجال تطوير الإعلام الآلي و ترتكز على نموذج CMM[3] والذي يتناول عدة مواضع مثل إقتناء البرمجيات Software acquisition وإدارة الموارد البشرية وهندسة الأنظمة. تهدف هذه الطريقة الى تشجيع المستعمل لها من وضع سيرورته تحت المراقبة مع تحسينها بصفة مستمرة. تقييم مستوى النضج يمر عبر 5 مستويات التالية:

- الأصلي: عوامل النجاح للمشاريع الغير محددة فالنجاح لا يمكن إعادته.
- إدارة: المشاريع تدار فوريا والنجاح يمكن تكراره.
- التحديد: سيرورة القيادة للمشاريع يتم وضعها بواسطة مقاييس وإجراءات وأدوات وطرق.
- الإدارة الكمية: نجاح المشاريع يمكن تقيمها وأسباب الفوارق يمكن تحليلها.
- التعظيم : إجراء التعظيم يبقى مستمر[4].

يقترح ميشال كمال[5] المقاربات الخاصة بإدارة أمن المعلومة و تشمل ثلاثة مقاربات و هي المقاربة الموجهة للمنتوجات و المقاربة الموجهة نحو إدارة المخاطر و المقاربة الموجهة نحو السيرورات[6].

فالمعايير والمراجع والطرق أو المناهج التي ذكرناها نضيف إليها كل من:

✓ BS[7] 7799
✓ [8]ISO 13335
✓ ITBPM[9]
✓ ITIL[10]
✓ [11]NIST 800-300
✓ [1]RFC 2196

[1] Objectives for business and Related Technology ,
[2] Capability Maturity Model Integration
[3] Capability Maturity Model
[4] Kamel Michel, opcit, p 76-89.
[5] Evaluation assurance Level.
[6] حميدوش أمحمد، مرجع سابق، ص 94، 97 و98.
[7] British Standard
[8] International Standardization Organization
[9] Information Technology Baseline Protection Manual
[10] Information Technology Infrastructure Library
[11] National Institute of Standards and Technology

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

- ✓ SSE-CMM[2]
- ✓ ITSEC[3]
- ✓ MOF / MSF[4]
- ✓ و دليل كل من PSSI[5] و TDBSSI[6]

لتوضيح أكثر عن هذه الطرق وأصحابها سوآءا كانت قد أصدرتها هيئات قياس عالمية أو مؤسسات رسمية أو قطاع خاص أو جمعيات نلخصها في الجدول التالي:

جدول رقم 2: القياسات الخاصة بالطرق ادارة الأمن المعلوماتي

الطريقة	تاريخ الإنشاء	صاحب الطريقة	دعم من	البلد	أدوات جتهزة	وضعية
EBIOS	1995	المديرية المركزية للأمن DCSSI	الحكومة	فرنسا	برمجية مجانا	
MELISA	-	المديرية العامة للجيش	الحكومة	فرنسا	-	تم التخلي عنها
MARION	1980	Clusif[7] نادي الفرنسي للأمن في الإعلام الآلي	جمعية	فرنسا		تم التخلي عنها
MEHARI	1995	CLUSIF	جمعية	فرنسا	برمجية Risicare	
octave	1999	Carnegie Mellon University	جمعية	الولايات المتحدة الأمريكية	برمجية للبيع	
Cramm	1986	Siemens	حكومة	بريطانيا	برمجية للبيع	
Sprint	1995	ISF	جمعية	بريطانيا	برمجية للبيع	
BS 7799	-	-	حكومة	بريطانيا	-	
ISO 17799	-		دولي			
ISO 13335	-		دولي			
ISO 15408			دولي			
SCORE	2004	Ageris Consulting	قطاع خاص	فرنسا	برمجية للبيع	
CALLIO	2001	CALLIO technologies	قطاع خاص	كندا	برمجية للبيع	
COBRA	2001	C&A Systems Security tilted	قطاع خاص	بريطانيا	برمجية للبيع	
ISAMM	2002	EVOSEC	قطاع خاص	بلجيكا	-	
RA2	2000	Aexis	قطاع خاص	ألمانيا	برمجية للبيع	

[1] Request For Comments
[2] Request For Comments
[3] Information Technology Security Evaluation Criteria
[4] Microsoft Operations Framework/ Microsoft Solutions Framework
[5] Politique de Sécurité des Systèmes d'Information
[6] Tableaux De Bord de Sécurité des Systèmes d'Information
[7] Club de la sécurité informatique Français

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

بغض النظر عن الطرق والمناهج التي ذكرنها والذي إهتم بها العديد من الباحثين والتي يجب أن تندرج ضمن سياسة الأمن بحيث بنائها يتطلب:

✓ تحديد مجموعة من أولويات الأمن التي يجب تلبيتها من أجل النظام (مثال معلومة مصنفة يجب ألا ترسل إلى مستعمل غير مؤهل بمعرفتها).

✓ إعداد مخطط التراخيص التي تعرض القواعد التي تمكن من تعديل حماية النظام (مثال حامل معلومة يمكن له إعطاء حق الولوج إلى هذه المعلومة لأي مستعمل [1].

كما أن المختصين يقترحون الأدوات الخاصة بالحماية و لا سيما التأمين علي الشبكة من خلال فريق التفاعل للاستجابة عن الحوادث الأمنية علي نظام الإعلام الآلي من حيث التسريح و الذي يهدف إلي التمكين بالقيام بأعمال شرعية أي منع مستعمل تنفيذ عمليات التي ليست مسموحة له [2] و من بين الطرق المستعملة للحماية الشبكة نشير إلي :

✓ التقطيع :(hachage) وظيفة التقطيع في إتجاه واحد (one way function) بحيث يولد بصمة حجمها ثابت إنطلاقا من رسالة ذات حجم معين. البصمة هي خصوصية النص ويجب أن يكون الإحتمال ضعيف حتى يكون لرسالتين نفس البصمة وتصميم وظيفة التقطيع (H)على الشكل التالي:

- نعرف M يسهل حساب البصمة H(M)
- نعرف H(M) يجب أن يستحيل إيجاد M
- نعرف H(M) يجب أن يستحيل إيجاد M الذي يختلف عن M و له نفس البصمة : H(M)=H(M') [3]

✓ الإمضاء ومراقبة السلامة (intégrité): الإمضاء يخدم سلامة المعلومات ويتحصل عليها من خلال تطبيق النص وظيفة توليد إمضاء بإستعمال مفتاح إمضاء (KS). مراقبة الإمضاء تكون بواسطة خوارزم التأكد من الإمضاء ومفتاح المراقبة (kv). في حالة تغير في النص أو إمضاء خوارزم المراقبة يعطي إجابة سلبية لضمان سلامة النص. هذه السلامة ترتكز على وظيفة توالد (génération)الإمضاء.

✓ المطابقات [4] (certificat) : المنطق السابق المطبق (الترميز و الإمضاءات ذات المفاتيح العمومية) تفترض صحة المفاتيح العمومية و لكن هذه المصداقية لا يمكن ضمانها في إستعمال الإنترنيت مثلا (يمكن مهاجم يغير المفتاح العمومي) و يمكنه قراءة البريد بانتحال الإمضاء و لتصدي هذا النوع من المهاجمين ثم إنشاء مكانيزم إضافي المطابقة الإلكترونية و التي تغطي دور التوثيق (authentification) للمرسل، ضمان سلامة (intégrité) الوثائق و عند الاقتضاء التاريخ و الساعة [5].

✓ الفاصل والحواجز النارية (cloisonnement & firewalls): الفصل مبدأ هام في الأمن بحيث يتم عزل كل ما لا يحتاج الإتصال مثال عزل أنظمة الإستغلال ويستحسن تخصيص المراكز حسب حساسية المعلومات بحيث لا تحتوي على المعلومات العمومية (غير مصنفة) ويجب أن تحتوي على المعلومات المصنفة. أما الحواجز النارية (par feux) تمكن من حراسة وحصر الولوج من الخارج (من الأنترنيت مثلا) وهو أحد الميكانيزمات لمراقبة الولوج التي يمكن أن ينفذ لتوطيد قواعد سياسية الأمن. يتضمن الحاجز الناري وظيفة غربلة (filtrage) بحيث يترك تمر إلى الحزمات (paquets) القادمة من بعض العناوين المرخصة أي رقم IP [6] و رقم الحمل

---

[1] Anas Abou El-KALAM , opcit , p 15

[2] Yves Deswarte, la sécurité des systèmes d'information et de communication, dans sécurité des réseaux et des systèmes répartis, Yves Deswarte & Ludovic Mé, eds, traité IC2, Hermès, ISBN : 02-7462-0770-2, octobre 2003, 264 p (cité dans Anas Abou El-KALAM , opcit , p 15).

[3] Anas Abou El KALAM , opcit , p 15.

[4] Anas Abou El KALAM , opcit , p 18-23

[5] حسب القياس الفرنسي x509 V3 المطابقة الإلكترونية يجب أن تحتوي بالخصوص على إسم سلطة المطابقة إسم ولقب الشخص، منظمته، عنوانه الإلكتروني، المفتاح العمومي، ومدة سيران المطابقة وكذلك الإمضاء الإلكتروني. هذا الإمضاء المحسوب على المعلومات التي تحتويها المطابقة وهي بصمة المعلومات المرمزة مع مفتاح الخاص لسلطة التي أعطت المطابقة.

[6] Identify prolocale

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والإجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

(Port) و التوجه نحو بعض العناوين المرخصة و يمكن أن يقدم وظائف تكميلية كترجمة العنوانين (NAT[1]) أو لعب دور الوكيل بالتنفيذ. ترجمة العناوين تمكن من إدارة فضاء خاص بعناوين شبكة داخلية مستقلة عن الشبكة الخارجية بحيث العناوين الداخلية غير معروفة من الخارج و تترجم إلى عناوين للخارج من طرف الحاجز الناري[2].

ثانيا: الحماية من حرب المعلومات

حسب GUICHARDAZ[3] يوجد أربعة إستراتجيات لمحاربة الجوسسة الصناعية و التي ترتب حسب أصناف التهديدات و الذي تتطبق عليه هذه الإستراتجية فالأولى تخص الفرد بحيث أن علي كل فرد من المفروض أن يحمي المعلومات التي بحوزته وقد تكون هذه المعلومات ذات طابع شخصي أو لها علاقة بالمنظمة. الإستراتجية الثانية تطبق على مديرية أو على مصلحة في المنظمة وتخص حماية المعلومة التي بحوزة مجموعة من الأفراد. الإستراتجية الثالثة ذات مجال أوسع وتخص المنظمة بإعتبارها مؤسسة والتي تعطي الطابع الرسمي للممارسة الحماية مع إتخاذ الإجراءات المضادة. و الإستراتجية الرابعة تخص المجموعة أي شبكة المنظمة من الوكالات و الفروع التابعة لها و الزبائن و المناولون.. إلخ.

حماية المعلومة ولا سيما المعلومة الإستراتيجية تتطلب الإهتمام كل من:

✓ الحماية من خلال الأفراد: بحيث يكون الفرد مركز الحماية والمعنى بحماية الأملاك وبالتالي حماية المعلومات يجب أن تدخل في التربية المدنية للأشخاص وهذا ما يتطلب وضع إستراتجية الحماية مع تحسين العلاقة مع كل أعضاء والإهتمام بمصلحة المجموعة.

✓ الحماية التي تقوم بها المنظمة أو المؤسسة: بحيث تستجيب إلى أربعة أسئلة أساسية: كيف يتم جمع المعلومة وكيف يتم حمايتها بمعنى يجب أخذ كقاعدة المخاطر الثلاثة الكبرى التي تهدد المعلومة: تحطيمها وتغيرها وتناولها (compromission) ثم كيف يتم إدارة المعلومة يوميا أين المعلومة ومن يحملها وكيف تنقل المعلومة من نقطة الجمع إلى التخزين.

✓ حراسة المعلومة المضادة Contre information و التي تعرف على أنها مجموع أعمال إتصال و التي بواسطة معلومة ذات علاقة بالموضوع و التي يمكن التأكد منها و بالتالي يمكن من تقليل أو إلغاء أو الرد ضد المحرض و الذي قام بالهجوم من خلال المعلومة و المعاومة المضادة[4]. المبدأ العام للمعلومة المضادة حسب (HARBULOT & JACQUES–GUSTAVE)هو إستغلال تناقص الخصم وهناك عدة مواصفات لفعالية حرب المعلومة والموجزة فيما يلي:

- لتكون ذات مصداقية المعلومة المضادة فيتم السعي إلى نقل المعلومة المفتوحة أو المبررة مع عدم التلاعب بها ويمكن التأكد منها بسهولة.
- أين وكيف ومتى وبأي حجم يتم نشر المعلومة؟ المعلومة المضادة هي قضية إستراتيجية وإدارة المعلومة.
- مهاجمة بصفة نظامية كل تناقضات ونقاط ضعف الخصم.
- مبرر الهجوم يكون قاطع إذا ما تثبت الوقائع بأدلة
- الإتصال مرتبط بالمثالية في البرهنة والإستعمال الماهر لصناديق الصدى العفوية Caisses des résonnances spontanées

الحماية و الأمن المعلوماتي التي تمارسه المنظمات يجب أن تدعمه مؤسسات الدولة لضمان دور نشاط الحماية بحيث أشار تقرير (Bernard Carayon) بأن سياسة الأمن الإقتصادي تحمي المحيط الإستراتيجي للاقتصاد

[1]Network adress translation
[2]Anas Abou ElKALAM , opcit , p 23
[3]GUICHARDAZ P. e les autres, l'infoguerre : stratégies de contre-intelligence économique, Dunod, 1999, p 126.
[4]Christian HARBULOT & JACQUES – GUSTAVE, manœuvre médiatique et compétition économique, Enjeux Atlantique, n° 16, 1998 ; p 16-19.

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

الوطني و بالخصوص القطاعات المفتاحية والأساسية في الإقتصاد[1] و حسب (Martinet & Marti) مجال الذكاء الإقتصادي يتضمن وضع إجراءات وتقنيات الأمن و هو المفهوم عند الفرنسيين أما بالنسبة للولايات المتحدة الأمريكية فالمفهوم الرسمي للأمن المعلوماتي يدخل في مجال الأمن الإقتصادي يتضمن ثلاثة محاور و هي الدعم للنشاطات الإقتصادية في الخارج ومحاربة الجوسسة الإقتصادية الأجنبية ومنع الممارسة الغير شرعية للمنظمات الأجنبية[2].

فدور الدولة يجب أن ينصب في المساعدة في إرساء والتحسيس على حماية المعلومة الاستراتيجية ولاسيما في المنظمات الصغيرة والمتوسطة على عكس المنظمات الكبرى والمتعددة الجنسيات لأنها قادرة على إدارتها بوحدها. الأمن هو قضية الجميع ولكن لدول دور أساسي ومن مهامه حماية الأفراد والمنظمات ومصالحة مما يتحتم وضع تنظيم والهيكلة لذلك.

وفي سياق الأمن المعلوماتي التي تشرف عليه الدولة نشير إلي تجربتين و سوف نهتم بالجانب التشريعي و التنظيمي أي الدور المنوط للمؤسسات الرسمية و المخول لها لعب مهمة الأمن المعلوماتي:

1-2 التجربة الفرنسية:

بحيث من الجانب القانوني ترتكز بالدرجة الأولي على التقنين الصادر من الاتحاد الأوروبي بحيث تم إنشاء وكالة أمن الشبكات والمعلومة التي أنشأها البرلمان الأوروبي تحت تنظيم 2004/ 460 بحيث تقدم هذه الهيئة للجنة الأوروبية مبادرات والمؤدية إلى إصدار توجيهات من طرف اللجنة الأوربية لدول الأعضاء في مجال التشريع والذي يخص أمن نظام المعلومات كما أن هاته الوكالة تميز بين المعلومة المصنفة دفاع والمعلومات الأخرى الحساسة الغير مصنفة. المعلومات المصنفة دفاع يعاقب عليها القانون الجبائي أما المعلومات الحساسة لا يوجد قانون خاص بها ولكن عدة قوانين تحدد أصناف المعلومات التي يجب حمايتها لأنها سرية كسر المهنة secret professionnel وسر المراسلات secret de correspondances وسر الحياة الشخصية.. الخ. أما بالنسبة لتشريع الفرنسي فنجد قانون الأهلية رقم 1443-2004 الخاص بحيث المادة 3 منه مخصصة للإدارة الإلكترونية لتأمين على التبادل الإلكتروني بين الإدارة والمستعملين والنصوص الخاصة بالتشفير كإحدى مركبات الأمن على نظام المعلومات مع تنظم استعمال وتقديم وتصدير المنتوجات الخاصة بخدمات التشفير والتي يخضعها القانون رقم 575-2004 للمراقبة.

أما في مجال التأمين على الاقتصاد الرقمي والذي يفرض التصريح والترخيص حسب الحالة للرسائل وخدمات التشفير وبالنظر لعدم نشر المراسم التنفيذية الخاصة به فالقانون السابق رقم 90-1170 يبقي ساري المفعول. كما أن النصوص الخاصة بالإمضاء الإلكتروني ومحاربة الجرائم السيبارنيتكية يعتبران إحدى مركبات أمن نظام المعلومات بحيث يمكن من التصديق للمرسل الوثيقة وضمانها وفق المادة رقم 230-2000 للمادة 1316 من القانون المدني للهيئات الرسمية والقانونية ويعرف الإمضاء الإلكتروني ومصداقيته حسب الشروط التي يحددها المرسوم 272-2001 والذي تكيف مع التعليمة الأوروبية رقم 1999/93/CE. أما القوانين الخاصة بالإجرام السيبارنيتكي نشير إلي القانون رقم 575-2004 و المواد من 323- 1 إلى 323-7 من القانون الجنائي و التي تعاقب كل مساس بأنظمة المعالجة الآلية للمعلومات و المادة 163-4 من القانون النقدي والمالي و التي تعاقب على صناعة أو حيازة أو تنازل على وسائل اعتلام آلي التي تمكن من الهجوم على البطاقات البنكية.

2-2 التنظيم الخاص بالتأمين على حماية أنظمة المعلومات:

تختلف الهيئات الفاعلة التي تشرف على سياسة التأمين على أنظمة المعلومات وهي:

[1]Philipe Clerc, intelligence économique : Québec, Royaume Unis, Suède, France cultures et pratiques comparées, Association Française pour le développement de l'intelligence économique, 2004 (sur le site : www.inforguerre.com et visité le 01/07/2009

[2]Didier Lucas & Alain Tiffreau , la dissuasion par l'information, École de guerre économique, group ESHSCA, 2000 (disponible sur le site de l'École : http://www.ege.fr/ et visité le 12/09/2009).

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والإجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

✓ الأمانة العامة للدفاع الوطني[1] بحيث وكلت لها مهام السهر على تناسق أعمال المنظمات في مجال امن منظومات الإعلام وبالخصوص المديرية المركزية لأمن علي أنظمة المعلومات[2] و التي ترافق الأمانة العامة لدفاع الوطني للإستجابة إلى هدفين رئيسين وهما ضمان أمن أنظمة المعلومة للدولة لإدارة الهياكل الحيوية و إنشاء شروط محيط ملائم للثقة التي تواكب تطور مجتمع الإعلام بفرنسا و أروبا. لهذه المديرية دور التعريف والتعبير عن سياسة الحكومة في مجال أمن أنظمة المعلومة ضمن اللجنة الوزارية المشتركة للأمن على أنظمة المعلومة[3] و التي تترأسها الأمانة العامة للدفاع الوطني و تقوم هذه المديرية بالوظائف التالية :

- ضمان وظيفة السلطة الوطنية لتنظيم في مجال امن أنظمة المعلومات من خلال تنظيم أشغال اللجنة وتحضير إجراءات لتقترحها الأمانة العامة للدفاع الوطني إلى الوزير الأول
- اقتراح ملفات وتراخيص للوزير الأول في مجال التشفير والإجراءات الخاصة بالتقييس والضبط والقيام بالإنذار واليقظة والإجابة عن الهجومات التي تمس أنظمة المعلومة والمساهمة في التكوين والتحسن. مع الإشارة إلي أن الوظيفة الأساسية هو التنسيق والتشاور بين الدوائر الوزارية

✓ وزارة الدفاع الوطني : لديها مسؤولية اخذ بعين الإعتبار أمن المعلومة للهيئات الخاصة و المعنية والمكاتب المركزية للأنظمة المعلومة كما لها دور السيطرة على سيرورة المنتوجات الحكومية الخاصة بالأمن العالي hautes sécurité

✓ وزارة الداخلية : في إطار مهامها تهتم من خلال حراسة الإقليم التحسيس ومحاربة الجريمة السيبارنيتكية

✓ وزارة الإقتصاد والمالية والصناعية : بحيث تساهم في تمويل الإبداع في مجال أمن أنظمة المعلومات لدى المنظمات من خلال مختلف الميكانيزمات المساعدة وبالخصوص عن طريق القرض الضريب في مجال البحث[4] Crédit impôt de recherche و الذي تتابعه المديرية العامة للمنظمات كما تشرف هذه المديرية على تمويل البحث والتطوير لا سيما في مجال الاتصالات والبرمجيات والمركبات و الأقطاب التنافسية (المناطق الصناعية) و نذكر برنامج أوبيدوم[5] كما تقوم الوكالة لتطوير الإدارة الإلكترونية[6] بتحفيز لتطوير أنظمة المعلومات التي تمكن من عصرنة الإدارة لتلبية حاجيات الجمهور و تقترح للوزير الأول رقمنة الإجراءات الإدارية الخاصة بعمليات أنظمة المعلومات و تطوير المعايير المرجعية المشتركة. وبالتنسيق مع مديرية المركزية للأمن علي أنظمة المعلومات مع وضع هياكل الثقة و الأدوات و الدلائل والمنهجية و خبرات EBIOS [7] أي التعبير عن حاجيات وتحديد أهداف الأمن مناهج إدارة المخاطر و بطاقات التعبير العقلانية للأهداف الأمن FEROS[8]

✓ اللجنة الوطنية للإعلام الآلي والحريات بإعتبارها هيئة مستقلة هدفها حماية الحياة الشخصية والحريات الفردية والعمومية فتهتم بسرية المعطيات وقد منح القانون المؤرخ في 6 أوت 2004 لهذه اللجنة مهمة إعطاء العلامة التجارية labellisation للمنتوجات والإجراءات.

✓ الدوائر الوزارية : كل وزارة تطبق إجراءات الأمن حسب القطاع و حاجيته وهذه الحرية تؤطرها تعليمات عامة وزارية مشتركة تحدد مسؤولية كل وزير ومطالب بتطوير على مستويات مشكل الأمن وتقرير المستمر لمستوى امن المنشآت و إحصاء – الحاجيات في مجال حماية أنظمة المعلومات والسهر على تلبيتها.

---

[1] المرسوم 67-96 المؤرخ في 29 جانفي 1996 المتعلق بصلاحيات الأمانة العامة للدفاع الوطني في مجال أمن انظمة المعلومة

[2] المرسوم رقم 69342 -2001 المحدد لصلاحيات المديرية المركزية لأمن نظم المعلومات.

[3] المرسوم رقم 69443 – 2001 اذي يحدد دور اللجنة الوزارية المشتركة للأمن على أنظمة المعلومة

[4] يخفض من ضريبة على الأرباح السنوية من خلال النافقات الموجهة إلى البحث في مجال التأمين علي أنظمة المعلومات و يناسبه مبلغ قرض ضريبة البحث.

[5] برنامج اوبيدوم في 1998 موجه للأمن و الذي يمكن من تطوير حلول تجارية ترافق تحرير التشفير و الاقتصاد الإلكتروني و إجراءات النقل اللاسلكي وحماية شبكات منظمات وأمن بطاقة شفرة السيلكون بحيث في 2004 خصص لهذا البرنامج مبلغ 4 مليون أورو وعرف نجاح بحيث ثم إيداع 45 ملف مبلغها يتطلب تمويل بما يعادل 22 مليون أورو.

[6] إنشائها بالمرسوم المؤرخ في 21 فبراير 2003 المنشور في الجريد الرسمية للجمهورية الفرنسية المؤرخة في 22 فبراير 2003.

[7] Expression des besoins et identification des objectifs de sécurités

[8] Fiches d'expression rationnelles des objectifs de sécurité au sens de ISO 15408

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والإجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (32) أبريل 2022
Volume (32) April 2022
IJOHSS

كما أن مديرية تحليل المعلومات وحماية المنشآت مكلفة بتطوير مخطط وطني للتأمين على الهياكل الحرجة ووضع جهاز يتجاوب مع الهجومات الخاصة بأمن أنظمة المعلومة الحرجة وضمان المساعدة التقنية للقطاع الخاص عند الحوادث التي تمس أنظمة المعلومات الحرجة وتنسيق نشر معلومة كما تنشر الإنذار و تشجيع البحث في هذا المجال.

خلاصة:

لحماية المعلومة الرقمية فإننا نوصي بتوفير البرمجيات التالية:

✓ برمجيات ضد الفيروسات مع اقتناء خدمة التحسين المستمر على الشبكة.

✓ برامج ضد الاختلاج Anti-spam

✓ التأمين البريدي بواسطة توفير التشفير لتفادي اعتراض الرسائل الإلكترونية سواء بإستعمال VPN : virtual privale Network و يستعمل لربط طرفين لنفس النظام معلومة وتفادي الاعتراض أو البرمجيات الخاصة بتشفير الملفات قبل الإرسال أو عند التخزين يضمن المعلومات في حالة ضياع او سرقة كمبيوتر الخاص المحمول.

✓ برمجيات الحواجز النارية firewall أو Pares feu بحيث وظيفة هذه البرمجيات مراقبة الربط بين شبكتين المطبقتان لسياسة الأمن مختلفة مع مراقبة كل التبادلات الرسمية ليخص سياسة الربط وقد تكون على شكل معدات عوض من برنامج تدمج مع النادل.

✓ برمجيات الإدارة الأكيدة التي تمركز الحقوق و الأسرار و تقييم تجهيزات الأمن وتسمى هذه البرمجيات بي security 3 A Software[1] ويمكن تلخصها بأنها برمجيات إدارة الولوج والهوية.

المراجع

1. حميدوش أمحمد، الذكاء الاقتصادي "فهمه و إنشاؤه و تأصيله و إستعماله"، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية و علوم التسيير، جامعة الجزائر 3، جانفي 2014،

2. محمد بن سعود آل سعود، تدفق المعلومات بين الحرية والأمن في بيئة العمل الحكومية، مؤتمر تقنيات المعلومات و الأمن الوطني، مجلة الاتصالات والعالم الرقمي، العدد 234، 2007 .

3. موضي بنت عبد المحسن الخميس، دور مراكز المعلومات في دعم القرار السياسي، مؤتمر حول تقنية المعلومات والأمن القومي، الرياض، المملكة العربية السعودية، 1-4 ديسمبر 2007.

4. François Jakobiak, François Jakobiak, l'intelligence économique en pratique, comment bâtir son propre système d'intelligence économique, Éditions d'organisation, 2ème Edition, France, 2001, p 235

5. Larivet Sophie, (2002), les réalités de l'intelligence économique en PME, thèse pour l'obtention de doctorat en Sciences de Gestion, Université de Toulon et du Var, 2002 (cité dans Ilhème Ghalamallah et les autres, Intelligence économique : proposition d'un outil dédié à l'analyse relationnelle, SciWatch Journal, Volume 3, Issue 2, 2008,

6. Philippe CLERC, Encyclopaedia Universalis, 1995.

7. Pierre LASBORDE, la sécurité des systèmes d'information: un enjeu majeur pour la France, rapport du 26 novembre 2005, la documentation Française,.

8. en.wikipedia .org/ wibi/Adware (visité le 12/02/2014).

9. Audrey KNAUF, caractérisation des rôles du coordinateur animateur : émergence d'un acteur nécessaire à la mise en pratique d'un dispositif régional d'intelligence

[1]Authen tification, Au torisation & Administration

DOI: 10.33193/IJoHSS.32.2022.395

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
2022 أبريل (32) العدد
Volume (32) April 2022
IJOHSS

économique, thèse de doctorat en sciences de l'information et de la communication, Université de Nancy 2, École doctorale langages, temps, Sociétés, France, 2007 .
10. Fabrice Frank, fondement d'une politique de sécurité globale des systèmes d'information au sein d'une grande entreprise, communication sur la gestion des risques, thèse de master en management des systèmes d'information et des technologies , École des Mines de Paris France, 2002.
11. ITSEC , Information Technology Security Evaluation Criteria, V 12, 136 p, office des Publications officielles des Communautés Européennes, Luxembourg, 1991 (cité dans Anas Abou El Kalam, Anas Abou El Kalam, patrons organisationnels et techniques pour la sécurisation des organisations virtuelles, thèse de doctorat en informatique, Université de Toulouse III, Paul Sabatier, France, 2008,
12. L.J Hoffman, smoking the bada chers : risk analysis in the age of micro–computer, Computer and Security, vol 8, p 299-302, 1989 (cité dans Elie BURSZTEIN, anticipation games, théorie des jeux appliqués à la sécurité des réseaux , thèse de doctorat en informatique, École Supérieure de Cachan France, 208, p 10.
13. Z A nastovski, risk analysis in computer network, a review, technical report, Center for computer security research, Wollongong NSW, Australia, 1993 (cité dans Elie BURSZTEIN, opcit.
14. Fabrice Frank, fondement d'une politique de sécurité globale des systèmes d'information au sein d'une grande entreprise : communication sur la gestion des risques, thèse de master en management des systèmes d'information et des technologies , École des Mines de Paris France, 20025.

DOI: 10.33193/IJoHSS.32.2022.395