آليات وقاية المعاملات الالكترونية في ظل حوكمة تكنولوجيا المعلومات

بوعقل مصطفى
جامعة جيلالي ليابس– سيدي بلعباس
bouakel.mustapha@outlook.fr

د.أونان بومدين
جامعة جيلالي ليابس– سيدي بلعباس
ounaneb@outlook.com

د. مباركي سمراء
جامعة جيلالي ليابس– سيدي بلعباس
sam_mebarki@yahoo.fr

ملخص:
أولت حوكمة تكنولوجيا المعلومات للأمان في البيئة الالكترونية اهتماما بالغا باعتباره المقوم الأساسي لنجاح المعاملات الاقتصادية، وقد شهد بمطلع الالفية الجديدة بعدا آخرا تجسد في استحداث الشركات العالمية لآليات وقائية تعمل على تشفير البيانات المحولة بين الاطراف وكذا وسائل لإثبات الهوية تشمل التوقيع الالكتروني والشهادات الرقمية، وانصب توجه بعض المهتمين الى معالجة أساليب وقاية أطر الدفع الالكتروني عن طريق تطوير نظام المعاملات الآمنة و بروتوكول الطبقات الآمنة، مع الأخذ بعين الاعتبار أساسيات حماية الشبكات المحلية للمؤسسات بواسطة الجدار الناري.

الكلمات المفتاحية:
حوكمة تكنولوجيا المعلومات – التشفير– التوقيع الالكتروني – الشهادة الرقمية – نظام المعاملات الالكترونية الآمنة – بروتوكول الطبقات الآمنة – الجدار الناري.

التصنيف: – ISSN1112-5969

Abstract:

Preventionmechanisms for electronic transactions under IT governance

Safety in the electronicenviron mentis one of the main concerns of IT governancesinceitisconsidered as the main basis for the success of economic transactions. The new age has witnessed the emergence of a new dimension where global corporatescreated protective mechanismsthatencryption the data transferredbetween parties, in

addition to means for identification such as electronic signature and digital certifications. Furthermore, research has been focused on improving the preventionmethods in the electronicpaymentusing a secureelectronictransactions and setting the secure socketlayersprotocol in addition to protecting the companies' local networks by use of firewalls.

Keywords:
IT Governance,Encryption,Electronic signature,Digital certificate,Secure electronic transaction,Secure socket layer Protocol,Firewall.
Classification: ISSN - 1112-5969

تمهيد:

أصبحت حوكمة تكنولوجيا المعلومات أحد أكبر اهتمامات منظمات الأعمال في الوقت الراهن،لاسيما في ظل الآثار التي أفرزتها المتغيرات البيئية الجديدة و ما يترتب عنها من مخاطر تتعلق بأمن و سرية المعلومات التي يتم تبادلها بين الأطراف أثناء إبرام صفقات المعاملات الالكترونية، فالمعلومات أثناء تدفقها عبر شبكة الأنترنت يمكن ان تحول ويقرأ محتواها خصوصا المعلومات المالية (أرقام الحسابات وأرقام بطاقات الائتمان)، كما يمكن أن تتعرض مواقع المؤسسات الى عمليات الاختراق و التخريب من طرف لصوص الانترنت "Internet Hackers" مما أدى الى ضرورة اللجوء الى مجموعة من الآليات والأنظمة التي توفر السرية، الأمن و الخصوصية.

إشكالية الدراسة:

في إطار البحث عن الخيارات والحلول التي تقي المتعاملين خطر التواجد في البيئة الالكترونية، وقصد ضمان الحماية الكافية لهم تنبثق معالم الإشكالية المصاغة في التساؤل الرئيسي التالي:

إلى أي مدى يمكنلحوكمة تكنولوجيا المعلومات خلق آليات كفيلة بوقايةالمعاملات الاقتصادية الالكترونية ؟

و هذا قادنا إلى تجزئة الاشكالية الأساسية إلى السؤالين الفرعيين التاليين:

- كيف يمكن لآليات الحماية الالكترونية الحد من مخاطر الاحتيال و القرصنة المعاصرة ؟
- هلمستقبل المعاملات الاقتصادية الالكترونية متوقف على مدىفعالية و نجاعة أساليب الوقاية التي تتيحهاحوكمة تكنولوجيا المعلومات ؟

فرضيات الدراسة:

- تقوم الهيئات العالمية المختصة في مجال المعلوماتية بابتكار و تطوير برمجيات الحماية الالكترونية وتحيينهاقصد التصدي لمخاطر الاحتيال و القرصنة المعاصرة.
- مستقبل التعامل الاقتصادي في الأوساط الالكترونية متوقف على مدى فعالية و نجاعة أساليب الوقاية الحديثة كون عنصر الأمان هو الركيزة الأساسية لقيام المبادلات التجارية و إجراء عمليات التسوية و بالتالي ضمان استمرارية حياة المنشأة.

و للإلمام بالموضوع و الإحاطة بجزئياته تطرقنا لدراسة المحاور التالية:

- حوكمة تكنولوجيا المعلومات
- التشفير و التوقيع الالكترونيين.
- الشهادات الرقمية و نظام المعاملات الالكترونية الآمنة.
- بروتوكول الطبقات الآمنة و الجدران النارية.

أهمية البحث:

إن مبدأ الأمان هو أول خطوة في المعاملات التجارية الالكترونية، فبدونه لا تقوى أطراف التبادل على التواجد في الأوساط الالكترونية لانعدام الثقة و غياب الحماية، الأمر الذي يجعلهم عرضة لمخاطر الغش و الاحتيال، و هذا ما يطرح مستقبل منظمات الأعمال أمام حافة الانهيار من جهة و إعاقة حركية التجارة و تراجع آليات

التواصل بين المتعاملين من جهة أخرى ما يعني بعبارة أو أخرى تحويل احداثيات المنظور الاقتصادي إلى أبعد الحدود، ما قد يتسبب في وضع مصير منظمات الأعمال على محك الانهيار.

1. مفهوم حكومة تكنولوجيا المعلومات:

1.1. تعريفحكومة تكنولوجيا المعلومات: تتعدد و تتنوع تعاريف حكومة تكنولوجيا المعلومات ،فقد قدم معهد حكومة تكنولوجيا المعلومات ITGI تعريفا ل حكومة تكنولوجيا المعلومات في سنة 2003 و هو "أن حكومة تكنولوجيا المعلومات هي مسؤولية مجلس الادارة، و الادارة التنفيذية، و هي جزءا مكملا لحكومة المشروعات و تتألف من القيادات و الهيكليات التنظيمية و العمليات التي تتضمن أن تكنولوجيا المعلومات المنظمة تساند و تبرز أهداف و استراتيجيات المنشاة "[1].

بينما يرى أحد الباحثين أنها: "وسيلة أو أداة فعالة في المنشاة من خلال خلق مرونة في تكنولوجيا المعلومات و في هيكليات و عمليات نظم المعلومات حيث ينظر إليها على أنها القدرة التنظيمية لرقابة تركيب و تطبيق استراتيجية تكنولوجيا المعلومات و تعتبر دليل للاتجاه المناسب بغرض تحقيق ميزة تناسبية للمنشاة "[2].

و من التعاريف السابقة يرى الباحثين إن حكومة تكنولوجيا المعلومات : "هي استخدام مجموعة من البالیات" من مبادئ و معايير وأهداف "في وضع و رسم سياسات و إجراءات لتحسين عمليات و أنشطة تكنولوجيا المعلومات و الرقابة عليه".

2.1– أهميةحوكمة تكنولوجيا المعلومات:

تعتبر حوكمة تكنولوجيا المعلومات جزء من حوكمة الشركات و امتداد لها، و تظهر أهمية حوكمة تكنولوجيا المعلومات من خلال دورها في تحقيق الأتي[3]:

- تطوير استراتيجية تكنولوجيا المعلومات و الشروع في الفحص التشغيلي و الاستراتيجي.
- تطوير و إدارة نظم تكنولوجيا المعلومات.
- تحديد الاساليب و الوسائل و العمليات المرتبطة بتكنولوجيا المعلومات .
- تحديد أفضل الممارسات في مجال التطور التكنولوجي.
- إدارة تنمية و تطوير التطبيقات تكنولوجية المعلومات.
- ضمان فعالية خدمات تكنولوجيا المعلمات لتوصيل الاستراتيجية لأقسام أنشطة الأعمال التي تؤدي إلى فعالية و كفاءة الإنتاجية التداخلية.
- تطوير مؤشرات الأداء الرئيسية.
- زيادة قدرة تكنولوجيا المعلومات لجدب الاختراعات و الابتكارات و توصيل المنافع المرجوة.

3.1 مقومات تطبيق حوكمة تكنولوجيا المعلومات:

تتمثل مقومات نجاح تطبيق حوكمة تكنولوجيا المعلومات في أي منشأة في ما يلي [4]:

- إدارة البنية التحتية لتكنولوجيا المعلومات تعود إلى القرارات المتعلقة بأنواع الأجهزة و البرامج وتشييد الشبكة و البيانات المستخدمة داخل المنشأة و المعايير الخاصة لإحراز و تطور أصولها الخاصة بتكنولوجيا المعلومات.
- الموائمة بين الاستراتيجية العامة للمؤسسة وخطط التشغيل اللازمة لتحقيق أهداف الاستراتيجية وبين الخطة الاستراتيجية لتقنية المعلومات[5].
- وضع خطة تشغيل لتكنولوجيا المعلومات .
- وضع خطة مالية وتمويلية لتكنولوجيا المعلومات .
- وضع إطار عام لتطبيق حوكمة تكنولوجيا المعلومات والرقابة عليها مأخوذا في الاعتبار ما تصدره جهات الرقابة والاشراف والتشريعات المنظمة للعمل بالمؤسسات واختيار البدائل العملية المطروحة مثل:COBIT

- لابد من القيام بتشكيل اللجان المتخصصة في توجيه تكنولوجيا المعلومات ووضع الاستراتيجية الخاصة بها ، ويتعين ان يكون مستوى هذه اللجان من اعضاء مجلس الادارة.

4.1 إدارة مخاطر تكنولوجيا المعلومات

تعتبر تكنولوجيا المعلومات من أهم المجالات التي تتعرض للعديد من المخاطر، وقد حددت لجنة التكنولوجياالمنبثقة من الاتحاد الدولي للمحاسبين IFAC مخاطر نظم تكنولوجيا المعلومات الى ثلاثة أنواع رئيسية من المخاطر هي[6]:

- مخاطر البنية التحتية لنظم تكنولوجيا المعلومات.
- مخاطر تطبيق تكنولوجيا المعلومات.
- مخاطر تكنولوجيا المعلومات الخاصة بأعمال المنشأة.

وفى ضوء ذلك أوصى مراجعي نظم المعلومات ان تنشئ المنشآت وحدة إدارية للرقابة والإشراف على تطبيق واستثمار تكنولوجيا المعلومات في المنشآت يطلق عليها لجنة الاشراف على تكنولوجيا المعلومات. كما أوضحت جمعيه مراجعة رقابة نظم المعلومات (ISACA) حاجة المنشآت لتكوين هذه اللجنة وفقاً للمعايير والقواعد التى أصدرتها الجمعية باسم " أهداف رقابة المعلومات وما يتعلق بها من تكنولوجيا The control objectives for Information and Related Technology (Cobit)وأوضحت فها دورها الفعال فى تطبيق الخطة الإستراتيجية لتكنولوجيا المعلومات للمنشاة والرقابة والإشراف والاستثمارات فها لتحقيق هدف المنشأة

كما انه تدعيما لإدارة مخاطر تكنولوجيا المعلومات فإنه لابد من ضرورة تبنى المنشاة تخصيص قسم أو إدارة – بحسب حجم الاستثمارفي تكنولوجيا المعلومات فى المنشأة– تكون مسئولة عن حماية أمن ونظم وتكنولوجيا المعلومات.

2. التشفير و التوقيع الالكترونيين

1.2 التشفير الالكتروني

1.1.2 مفهومالتشفير الالكتروني:

التشفير هو عملية دمج المعلومات في شفرة سرية غير مفهومة ثم فك هذه الشفرة بعد وصولها الى وحدة خدمة الويب الامنة ، أي ان التشفير هو استبدال مستند او رسالة باستخدام برنامج معين، و لهذا تنطوي عملية التشفير على تحويل النصوص البسيطة الى رموز (حروف، ارقام، اشارات) قبل ارسالها الى مستقبلها شريطة ان يكون لهذا الاخير القدرة على حل الشفرة و تحويل الرسالة الى صيغتها الاصلية باستخدام مفتاح التشفير[7].

2.1.2. طرق التشفيرالالكتروني:

1.2.1.2 التشفير باستخدام المفتاح المتماثل (المفتاح السري):

يعتمد نظام التشفير المتماثل او المتناظر symmetriccryptography على استخدام نفس المفتاح من طرف مصدر الرسالة والمرسل إليه للقيام بتشفير الرسالة و إعادة فك رموزها[8] و ذلك وفقا للخطوات التالية :

- في هذا النظام يتم استخدام المفتاح الخاص (السري) المستند الى وضع رياضة معقدة (خوارزميات) في عملية استبدال البيانات برموز وحروف بغرض الحصول على رسالة مشفرة.
- يقوم المستقبل بعد تلقي الرسالة المشفرة بحل الرموز ، و ذلك باستخدام نفس المفتاح الخاص (كلمة المرور) الذي يملكه المرسل حيث انه تم الاتفاق مسبقا بين الطرفين على كلمة المرور التي تقوم برمجيات التشفير بتحويلها الى ثنائي (اضافة الى رموز اخرى) هو المفتاح الخاص .

- بعد استخدام المستقبل لكلمة المرور بتشكيل المفتاح الذي يقوم بتحويل الرسالة المستقبلة من صورتها المرمزة غير المقروءة و غير المفهومة الى صورتها الاصلية الواضحة .
- ان عدم استغراق هذا النظام لوقت طويل و جهد كبير لتشفير encryption و فك تشفير البيانات decryption، ساهم كثيرا في حماية الرسائل المتنقلة من الاطلاع عليها ، الا انه يعترض استخدامه مشكلة امن تبادل المفتاح السري فهو عرضه للسرقة بسبب عدم توفر وسيلة مؤمنة و خاصة لنقله، كما انه في حالة تعامل المرسل مع عدد كبير من المستقبلين يتوجب عليه امتلاك الكثير من المفاتيح الخاصة بكل واحد منهم، اما اذا فضل المرسل استخدام مفتاح واحد فقط مع عدد من المستقبلين فان ذلك يؤدي الى شيوع المفتاح والإخلال بمبدأ السرية . ومن أمثلة ذلك: AES،IDEA، Blowfish

2.2.1.2 التشفير باستخدام المفتاح اللامتماثل (المفتاح العام) :

أو ما يعرف بالتشفير اللامتماثل Asymmetric) (Cryptography تم تطوير هذا النظام في السبعينات في بريطانيا وكان استخدامه حكراً على قطاعات معينة من الحكومة. ويعتمد في مبدأه على وجود مفتاحين وهما المفتاح العام Public key والمفتاح الخاصPrivet key، حيث أن المفتاح العام هو لتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل. المفتاح العام يرسل لجميع الناس أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد. فمن يحتاج أن يرسل لك رسالة مشفرة فإنه يستخدم المفتاح العام لتشفيرها ومن ثم تقوم باستقبالها وفك تشفيرها بمفتاحك الخاص[9]،ومن أمثلة ذلك: PGP، DSA.

إن ارتكاز نظام التشفير اللامتماثل على مبدأ عدم نشر المفتاح الخاص للجميع ، ساعد على توفير

حماية كبيرة للرسائل من التطفل عليها ، الا ان هذه السرية تتطلب الكثير من الوقت و الجهد والمعدات المعقدة لإجراء عملية التشفير وفكها مما يجعل هذا النظام جد بطيء و مكلف مقارنة بالنظام السابق.

3.2.1.2.المزج بين اسلوبي استخدام المفتاح المتماثل و المفتاح العام : يهدف هذا النظام الى تفادي عيوب النظامين السابقين من خلال ضمان قدر كبيرمن الامن و الحماية للبيانات باقل تكلفة و في اقصر وقت، و يستطيع هذا النظام تحقيق هدفه من خلال الجمع بين المفتاح المتماثل والمفتاح العام.

2.2. التوقيع الالكتروني:

تعتبر الكتابة على الورق اهم وسيلة لإثبات التصرفات القانونية و لا يتم الاعتراف بصحة المستند او الورقة الا اذا ارفقت بتوقيع شخصي يبين نسبها الى موقعها ، مما زاد من اهمية التوقيع الذي يميز هوية الموقع و شخصيته.

الا انه مع التطورات الراهنة في جميع مجالات حياتنا ، اصبح التوقيع اليدوي عقبة من المستحيل تكيفها مع التكنولوجيا الحديثة و خاصة مع تعاملات التجارة الالكترونية ، مما ادى الى ضرورة ظهور توقيع جديد يتماشى مع مقتضيات العصر الحديث و هو ما يصطلح عليه " التوقيع الرقمي"

1.2.2.تعريف التوقيع الالكتروني:

عرفت المادة (2/ا) من القانون النموذجي المتعلق بالتوقيعات الالكترونية و الذي و ضعته لجنة الامم المتحدة لقانون التجارة الدولية سنة 2001 التوقيع الالكتروني بانه "بيانات في شكل الكتروني مدرجة في رسالة بيانات او مضافة اليها او مرتبطة بها منطقيا، و يجوز ان تستخدم لتعيين هوية الموقع بالنسبة الى رسالة البيانات و بيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"[10].

اي ان التوقيع الالكتروني يتمثل في حروف و ارقام و اشارات مجموعة في ملف رقمي صغير يساعد على تمييز هوية الموقع و شخصيته دون غيره و بانه هو من قام بإجراء المعاملة و تنفيذها .

2.2.2.أنواع التوقيع الإلكتروني:

1.2.2.2.التوقيع الرقمي أو الكودي Digital Signature

وهو عبارة عن عدة أرقام يتم تركيبها لتكون في النهاية كودا يتم التوقيع به ويستخدم هذا في التعاملات البنكية والمراسلات الإلكترونية التي تتم بين التجار أو بين الشركات وبعضها ، ومثال لذلك بطاقة الائتمان التي تحتوى على رقم سرى لا يعرفه سوى العميل ، ويعد هذا النوع وسيلة آمنة لتحديد هوية الشخص الذى قام بالتوقيع من خلال الحاسب الالى[11].

2.2.2.2.التوقيع البيومترى Biometric Signature

ويقوم على أساس التحقق من شخصية المتعامل بالاعتماد على الصفات الجسمانية للأفراد مثل البصمة الشخصية ، مسح العين البشرية التعرف على الوجه البشرى ، خواص اليد البشرية ، التحقق من نبرة الصوت ، والتوقيع الشخصي، ويتم التأكد من شخصية المتعامل عن طريق إدخال المعلومات للحاسب أو الوسائل الحديثة مثل التقاط صورة دقيقة لعين المستخدم أو صوته أو يده ويتم تخزينها بطريقة مشفرة في ذاكرة الحاسب ليقوم بعد ذلك بالمطابقة . ويعترى هذا النظام العديد من المشاكل منها أن صورة التوقيع يتم وضعها على القرص الصلب للحاسب ومن ثم يمكن مهاجمتها أو نسخها بواسطة الطرق المستخدمة في القرصنة الإلكترونية ، كذلك عدم إمكانية استخدام هذه التقنية مع جميع الحاسبات المتوفرة ، ويحتاج هذا النوع من التوقيع الى استثمارات ضخمة لتمكين مستخدمي الشبكة الإلكترونية من استخدام الخصائص الذاتية لشخص الموقع في التوقيع الإلكتروني[12].

3.2.2.2.التوقيع بالقلم الإلكتروني PEN-OP

يقوم هنا مرسل الرسالة بكتابة توقيعه الشخصي باستخدام قلم إلكتروني خاص على شاشة الحاسب الألى عن طريق برنامج معين ويقوم هذا البرنامج بالتقاط التوقيع والتحقق من صحته ، ولكن يحتاج هذا النظام الى جهاز حاسب آلي بمواصفات خاصة ويستخدم هذا بواسطة أجهزة الأمن والمخابرات كوسيلة للتحقق من الشخصية .وهذا النوع افضل من التوقيع اليدوي والذى يتم على شاشة جهاز الكمبيوتر أو على لوحة خاصة معدة لذلك باستعمال قلم خاص عند ظهور المحرر الإلكتروني على الشاشة ، وهذا النوع لا يتمتع بأي درجة من الأمان كذلك لا يتضمن حجية في الإثبات[13].

3.الشهادات الرقمية و نظام المعاملات الآمنة

1.3.الشهادات الرقمية

لطالما تعرضت معاملات التجارة الالكترونية الى اشكال عديدة من الخداع و انتحال الشخصيات و لكي يتم تجنب هذا الخداع لابد من التحقق من هوية الاطراف المتبادلة للمعلومات و هذا باللجوء الى شهادات رقمية تؤكد شخصية المتعاملين .

1.1.3.مفهوم الشهادات الرقمية:هي وثيقة رقمية تحتوي على مجموعة من المعلومات التي تقود إلى التحقق من هوية الشخص أو المنظمة أو الموقع الإلكتروني و تشفر المعلومات التي يحويها جهاز الخادم (server) عبر ما يسمى بتقنية.(SSL Layer sockecSsecurS) يمكننا تشبيه الشهادة الرقمية بجواز سفر أو وثائق اعتماد رقمية تتم أثناء الاتصال بين الخادم (server)و العميل (client) فحينما يريد العميل ارسال معلومات تتصف بالسرية أو الحساسية يقوم متصفح الانترنت و بشكل آلي بالدخول إلى جهاز خادم (server) خاص للتأكد من هوية الجهة التي يرغب في إرسال المعلومات إليها و التالي يضمن الحصول على قناة اتصال آمنة[14]، و بهذا تساعد الشهادة الالكترونية صاحبها على تحقيق شخصيته الالكترونية و اثبات صحة كافة معلوماته و ضمان صدق العملية المطلوبة ، وهو ما يؤدي الى ضمان امن التعاملات التجارية و الفردية و بالتالي تطور و انتشار التجارة الالكترونية .

و تتضمن الشهادة الرقمية مجموعة من البيانات و المعلومات الالكترونية و التي قامت هيئة المواصفات القياسية العالمية iso بتحديدها و فقا للمعيار X-509 كالاتي[15] :

- بيانات عن المرسل تحدد هويته.
- نسخة من المفتاح العام للمرسل و توقيعه الرقمي.
- رقم تسلسلي للشهادة و تاريخ انتهاء صلاحيتها.

إضافة إلى :الخوارزمية المستخدمة لإنشاء التوقيع – اسم الجهة المصدرة للشهادة (هيئة التوثيق) – الغرض من استخدام المفتاح العام – الإصدار – خوارزمية بصمة الإبهام – بصمة الإبهام[16]

إن تعدد اطراف التجارة الالكترونية أدى الى ضرورة ايجاد انواع متعددة من الشهادات الرقمية تتوافق مع متطلبات كل طرف، فهناك الشهادات الرقمية الممنوحة للأفراد و المرفقة بمتصفحات الويب (Netscape ;Internet explorer) و هناك الشهادات الالكترونية الخاصة بالمؤسسات و التجار و الموجودة على مستوى خادم الويب والتي تضمن الوجود الفعلي لهدا الموقع و النوع الاخير هي شهادات التوقيع الالكتروني المستعملة لتأكد هوية صاحب الرسالة و اثبات صحة توقيعه و من بين اهم الهيئات المصدرة لهذا النوع من الشهادات :Verisign and digital signature trust

2.1.3.أهمية الشهادات الرقمية:

تساهم الشهادات الرقمية في تطوير التجارة الالكترونية بشكل كبير من خلال تأكيدها لهوية الطرفين و ضمانها لسرية المعاملات باستخدام تقنية التشفير حيث تحتوي كل شهادة على مجموعة من البيانات و المعلومات الموقعة بالمفتاح العام لصاحب الشهادة و كذلك المفتاح الخاص للهيئة المصدرة لهذه الشهادة فاذا نجح المستقبل في فك شفرة الشهادة باستخدام المفتاح العام للهيئة هذا يؤكد بان الهيئة الموقعة على الشهادة هي نفسها التي اصدرتها .

2.3. نظام المعاملات الالكترونية الامنة – 'SET' Secure Electronic Transaction

ان المشكل الرئيسي الذي تعاني منه التجارة الالكترونية هو مشكل تامين الدفع و الاخطار التي قد تترتب عنه، فالدفع الالكتروني باعتباره عملية مصرفية متعددة الاطراف و مفتوحة على فضاء دولي يمكنه ان يتعرض الى صور عديدة من الاعتداءات و التي تخلق لدى المشتري هاجس ضمان و تامين عملية شراء السلع عبر الانترنت ، كذلك للبائع الذي يرغب في ضمان قدرة الزبون على التسديد و لذلك تم التفكير في اللجوء الى وسائل امن حديثة قادرة على جعل الدفع اكثر فعالية و اكثر سرية و كذلك اكثر قدرة على حماية المستهلك و ضمان حقوق البائع، و من بين اهم هذه الوسائل نظام المعاملات الالكترونية الامنة « SET »

1.2.3.تعريف نظام المعاملات الالكترونية الامنة :

هو عبارة عن بروتوكول طورته مجموعة كبيرة من الشركات العالمية للائتمان كفيزا و ماستر كارد و وظيفته الاساسية هي توفير الامان لمدفوعات البطاقات المصرفية (الائتمانية) اثناء عبورها الانترنت بين حاملي البطاقات والتجار و البنوك[17]

و يستطيع هذا البروتوكول ضمان امن المعاملات المالية للبطاقات الائتمانية من خلال اصدار شهادات رقمية للمستهلكين و التجار تشهد بصحة هويتهم اثناء قيامهم بمعاملات التجارة الالكترونية

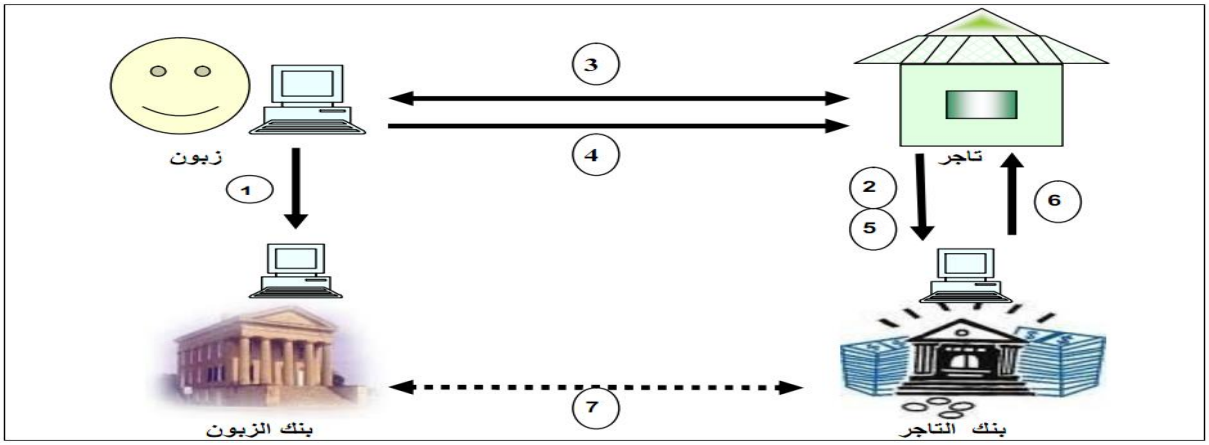
و يتم الاحتفاظ بهذه الشهادة في برمجيات المحفظة الالكترونية و التي تحتوي بالإضافةإلى شهادة "SET" معلومات أخرى مثل رقم البطاقة الائتمانية و تاريخ انتهائها حيث يتم تخزين هذه المحفظة على كمبيوتر المستخدم ليتم استعمالها للقيام بعملية الدفع عبر الانترنت في اي وقت، و يسعى هذا البروتوكول الى تحقيق مجموعة من الاهداف تتمثل في :

- تامين سرية المعلومات الخاصة بالدفع من خلال تقنية التشفير
- المعلومات المحولة تكون كاملة و غير قابلة لاي تغيير بفضل استخدام التوقيع الالكتروني
- تحديد هوية صاحب البطاقة و التاجر فالشهادات الالكترونية تضفي الكثير من الشرعية و الموثوقية على الطرفين و تدل ان البنك قد تحقق من شخصيتهما

2.2.3.مبدأ عمل نظام المعاملات الالكترونية الامنة :

يمكننا توضيح المراحل التي يتم بها استخدام نظام بروتوكول الحركات المالية الامنة من خلال الشكل:

الشكل (01) : مبدأ عمل نظام المعاملات الالكترونية الامنة



المصدر : جمال مزغيش، "التجارة الالكترونية على شبكة الأنترنت، دراسة حالة توجه المؤسسات الجزائرية نحو التجارة الالكترونية"، مذكرة ماجستير في العلوم الاقتصادية، جامعة الجزائر، 2002، ص101.

1) يشترك الزبون لدى احدى البنوك او المؤسسات الائتمانية بغية الحصول على برنامج خاص ببروتوكول الحركات المالية الامنة (هو برنامج المحفظة الالكترونية التي تحتوي على البطاقة الائتمانية و شهادة الكترونية)

2) يفتح التاجر ايضا حسابا لذى احد البنوك و يحصل على برمجيات لاستخدام بروتوكول set (تشمل هذه البرمجيات شهادة set و المفتاح العام)

3) يزور المشتري موقع البائع الذي يتعامل ببروتوكول set و يحدد حاجياته كما يستعمل الزبون المفتاح العام للتاجر من اجل تشفير معلومات طلب الشراء (الاصناف المطلوبة و الكميات و القيمة)

4) يستخدم الزبون المفتاح العام للتاجر من اجل تشفير معلومات الدفع (رقم بطاقة الائتمان و القيمة المدفوعة و اسم البائع) كما يستخدم هذا الزبون محفظته الالكترونية لإرسال المعلومات المالية المشفرة و الشهادة الالكترونية الى البائع .

5) يفك التاجر تشفير معلومات طلب الشراء باستخدام مفتاحه الخاص و يقوم بتوجيه المعلومات المالية المشفرة الى البنك او شركة الائتمان .

6) يتحقق البنك من هوية البائع و المشتري (باستخدام الشهادات الرقمية) و يعالج معلومات الدفع و يرسل رسالة الموافقة على الصفقة الى البائع ليقوم هذا الأخيربإتمام معاملات الصفقة و شحن البضاعة .

7) تتم عملية المقاصة بين بنك التاجر و بنك المشتري .

4.بروتوكول الطبقات الامنة و الجدران النارية

1.4.بروتوكول الطبقات الامنة"SSL"– Secure Socket Layer

ان الرغبة في استعمال بروتوكول تشفير يجمع بين الامان و البساطة و لا يتطلب تجهيزات خاصة للمشتري دفع المختصين الى تطوير بروتوكول الطبقات الامنة لتحقيق هذا الهدف .

1.1.4.تعريف بروتوكول الطبقات الامنة:

ان بروتوكول SSL هو بروتوكول تشفير رزم البيانات و يعمل ضمن متصفحات الويب (WEB BROWSER) من اجل منع اعتراض البيانات و المعلومات التي يجري ارسالها عبر الانترنت في اي نقطة اثناء انتقال هذه البيانات و المعلومات[18] .

و يتميز هذا البروتوكول بان عملية بث المعلومات تتم بأمان بين المتصفح و الخادم دون اي حاجة لتدخل المرسل لتشفير البيانات المتبادلة وكل ما على المرسل فعله للاستفادة من بروتوكول SSL هو استخدام متصفح امن و زيارة موقع امن و الذي يبدا عنوانه بـ (securehttps)بدلا من http و الذي يحتوي كذلك على مفتاح أو قفل مغلق أسفل الشاشة[19].

2.1.4.مبدأ عمل بروتوكول الطبقات الامنة:

يقوم مبدا عمل بروتوكول SSL على تأسيس قناة اتصال امنة و منفصلة للرسائل و هي بمثابة طبقة ارسال خاصة ووسيطة تربط بين بروتوكول التحكم بالنقل و بروتوكول http و لهذا يسمى بروتوكول الطبقة الامنة و تمر عملية استخدام بروتوكول الطبقات الامنة لبث المعلومات بأمان عبر الانترنت بالخطوات التالية :

- يتصل المتصفح بخادم ويب امن و الذي يبدأ عنوانه بـhttps.
- يتبادل المتصفح و الخادم معلومات التعريف التي تتضمن تفاصيل الصلاحيات (الشهادات الرقمية قدرات التشفير).[20]
- يتحقق المتصفح من الشهادة الرقمية للخادم.
- يقوم المتصفح بإنشاء مفتاح سري جديد لتشفير المعلومات المتبادلة بين الطرفين.
- يقوم المتصفح بتشفير المفتاح الجديد باستخدام المفتاح العام للخادم و يرسله لهذا الاخير الذي يقوم بفك التشفير باستخدام مفتاحه الخاص ليتمكن من التعرف على هذا المفتاح الجديد ولا يستطيع الخادم والمتصفح استخدام المفتاح السري للتبادل الا في جلسة واحدة.

2.4.الجدران النارية

ان انشاء المؤسسة لموقع على شبكة الانترنت يعني انفتاحها على العالم الخارجي و تعرض معلوماتها الداخلية الى العديد من عمليات التطفل و التخريب و اول خطوة تقوم بها المؤسسة لمنع دخول الزوار غير المرغوب فيهم الى موقعنا ، هي وضع برنامج واقي لمراقبة محاولات النفاد الى النظام الداخلي للمؤسسة يطلق عليه : الجدران النارية أو حوائط المنع.

1.2.4.ماهية الجدران النارية :

هي عبارة عن برمجيات هدفها الأساسي تامين الحماية الكافية لمعلومات الشركة و القضاء على كل عمليات الاختراق و التدمير التي تتعرض لها خوادم الويب، من خلال إقامة حاجز بين شبكة الانترنت و الشبكة الداخلية للمؤسسة ، ليقوم هذا الحاجز بتصفية و فحص كل عمليات الدخول و الخروج إلى الشبكة لمنع دخول المستخدمين غير المصرح لهم و غير المسجلين و لتجنب خطر الفيروسات و البرامج الداخلية .

2.2.4.طرق الحماية باستخدام حوائط المنع :

تقوم حوائط المنع بإدارة عملية النفاذ إلى الموقع أو الشبكة من خلال ثلاث طرق أساسية :

1.2.2.4.طريقة اتاحة العام و غلق الخاص :

عندما تتخذ المؤسسة قرار إنشاء هذا النوع من حوائط المنع فانها تقوم بتقسيم معلوماتها و بياناتها إلى معلومات عامة و معلومات سريةفالمعلومات العامة يتم وضعها على خادم يقع خارج جدار النار بهدف تمكين جميع الأشخاص من الاطلاع عليها ، أما المعلومات السرية فتوضع على خادم أخر يقع على الجدار الناري لمنع جميع محاولات الوصول إليها و تتعلق هذه المعلومات بتطبيقات و قواعد بيانات المؤسسة .

2.2.2.4.طريقة حوائط المنع المزدوجة :

يحول هذا الجدار المزدوج دون وصول الطلبات المشكوك فيها من الانترنت الى الخادمين العام و الخاص مباشرة ، فيتم وضع خادم الملفات العام بعد الجدار الناري الاول ، و يوضع خادم الملفات الخاص بعد الجدار الناري الثاني لترشيح و تصفية كل الرزم الداخلية و الخارجية من الشبكة و بهذا يتم توفير حماية كاملة لجميع معلومات المؤسسة العامة منها و الخاصة .

3.2.2.4.طريقة الفصل المطلق للخادمات :

و يتم وفقا لهذه الطريقة الفصل التام بين كل من خادم الملفات العام و خادم الملفات الخاص ، بحيث يكون الخادم الاخير بمثابة حاسب الي مستقل بذاته يعمل بنظام تشغيل امن يحول دون الدخول الى الملفات الخاصة بالمنظمة[21].

5.جهود الجزائر في إطار ترقية حوكمة تكنولوجيا المعلومات:

رغبة في زيادة التكامل مع المجتمع الاقتصادي العالمي بذلت الجزائر جهودا مكثفة نحو بناء إطار مؤسسي لحوكمة تكنولوجيا المعلومات حيث عملت على توفير مناخ استراتيجي لتفعيل بيئة الأعمال وانفتاحها الدولي، وفي سبيل تحقيق ذلك عمدت إلى إتباع منهجية عمل مدققة مرفوقة بجملة من الإجراءات الهادفة إلى تنمية هذا المجال والارتقاء به إلى مستوى العالمية.

1.5.المنجية المتبعة في إطار الخدمات الالكترونية[22]:

- العمل على مضاعفة المواقع الالكترونيةذات النمط المؤسسي.
- إنشاء أسس الحوكمة الوطنية.
- توفير كل الظروف الملائمة في مجال إنتاج البرمجيات وضمان وسائل الاتصال الآمن.
- تعزيز البنية الأساسية للاتصالات ذات نوعية وأمان وتستجيب للمقاييس الدولية.
- تطوير الكفاءات البشرية: إعادةالنظرفي برامج التعليم العالي والتكوين المهني في مجال تكنولوجيات الإعلام والاتصال.
- إنشاء لجنة المصادقة الإلكترونية.
- تثمين التعاون الدولي.

كما عمدت الجزائر في نفس الصدد على برمجة خطة عمل تقتضي مايلي[23]:

- تحديد رؤية وطنية للانضمام إلى مجتمع المعلومات ورزنامة عمل خاصة بالاستخدام الواسع لتكنولوجيا المعلومات والاتصالات الجديدة، والتي اعتمدت في عام 2002 من قبل الحكومة.
- تعزيز الإطار المؤسسي للسياسة العامة لتكنولوجيا المعلومات والاتصالات من خلال إنشاء وزارة محددة، والتحرير الكامل لقطاع الاتصالات.

2.5.إجراءات تحسين حوكمة تكنولوجيا المعلومات في الجزائر:

قامت الجزائر في سنة 2009، بإصدار "ميثاق الحكم الراشد للمؤسسة في الجزائر" والذي أشرفت على تسطيره مجموعة عمل حوكمة الشركات متعددة الأطراف[24]، كما أطلقت مركز "حوكمة الجزائر" لمساعدة الشركات الجزائرية على الالتزام بمواد الدليل واعتماد أفضل ممارسات حوكمة الشركات الدولية، ويعتبر إطلاق المركز فرصة جديدة لمجتمع الأعمال لإظهار التزامه بتحسين البيئة الاقتصادية في الجزائر وتحسين قيم الحوكمة الديمقراطية بما فيها الشفافية، والمساءلة، والمسؤولية[25].

وقد استهلت الجزائر تقنين التصديق الالكتروني بالمرسوم التنفيذي 07-162 المؤرخ في 30 ماي 2007 الصادر في الجريدة الرسمية العدد 37 لسنة 2007 والذي نظم نشاط التصديق الالكتروني من خلال إخضاعه إلى نظام الترخيص الوارد في المادة 39 من القانون 2000-03 المؤرخفي 5 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية، حيث نصت المادة03 من المرسوم التنفيذي 07-162 على أن "عملية اعداد واستغلال خدمات التصديق الالكتروني مرهونة بمنح ترخيص تسلمه سلطة ضبط البريد والاتصالات السلكية واللاسلكية"[26].
كما قامت الجزائر بإصدار القانون 15-04 المؤرخ في أول فبراير 2015 الصادر في الجريدة الرسمية العدد 06 لسنة 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونين، والذي تناول آليات التشفير وشهادات التصديق، وكذا السلطات المخول لها تنظيم وتسيير هذا المجال، فضلا عن توضيح النظام القانوني لتأدية خدمات التوقيع الالكتروني[27].

كما تم وضع ميثاق لتأمين الأنظمة والبيانات وتوزيعها على نطاق واسع من خلال[28]:

- إجراء حملة توعية لفائدة الإطارات المسؤولة على أنظمة المعلوماتية وكذا المستخدمين.
- إنشاء مواقع مرآة للأنظمة الحساسة.
- وضع إجراءات خاصة بعمليات الحفظ / الأرشفة والاسترجاع في حالة الطوارئ.
- وضع استراتيجية تكوين لفائدة المهندسين في إدارة وتأمين الأنظمة المعلوماتية المنجزة.

إعداد نص قانوني لحماية البيانات الشخصية.لقد تركت المجهودات التي بذلتها الجزائر قصد ترقية حوكمة تكنولوجيا المعلومات دفعة محسوسة في مجال تفعيل بيئة الأعمال، بالرغم من ابتعادها نسبيا عن المستوى العالمي حسب التقرير المصرح به من طرف البنك العالمي لسنة 2015[29]، الأمر الذي يستلزم تكريس المزيد من الاهتمام وتوحيد المساعي على أمل الوقوف مستقبلا على حوكمة ناجعة في مجال تكنولوجيا المعلومات خصوصا وقطاع المؤسسات والشركات عموما.

خاتمة:

كانت هذه بعض النصائح التي نراها ضرورية لنتفادى جميعا شر الوقوع في عمليات النصب و الإحتيال الموجودة في شبكة الانترنيت و التي أصبحت شائعة و متعددة الأشكال والأساليب ، حيث يستخدم المحتالون مواقع انترنت مزيفة، أو رسائل مضلّلة عن طريق البريد الالكتروني، وذلك بتقليد العلامات التجارية والشركات الموثوق بها، من أجل سرقة معلومات شخصية، مثل: أسماء المستخدمين، وكلمات السرّ، وأرقام بطاقات الائتمان ومعلومات الفواتير.

نتائج اختبار صحة الفرضيات:

- تقوم الهيئات العالمية المختصة في مجال المعلوماتية بتطوير برمجيات الحماية الالكترونية عن طريق البحث عن الثغرات في الأنظمة والتطبيقات التي قد تفتح المجال للقراصنة للممارسة أعمال غير شرعية و استخدام أساليب تضليلية للاعتداء على أمن وخصوصية المعلومات الشخصية، وفي هذا الصدد تقوم هذه الهيئات بإدراك النقائص و تحيين البرامج قصد مجاراةمخاطر الاحتيال و الغش المعاصرة، وبالتالي فالفرضية الأولى صحيحة.
- مستقبل التعامل الاقتصادي في الأوساط الالكترونية متوقف على مدى فعالية و نجاعة أساليب الوقاية الحديثة كون عنصر الأمان هو الركيزة الأساسية لقيام المبادلات التجارية و إجراء عمليات التسوية، فقيمة المعلومات التي تحافظ المنشآت على سريتها تعكس أبعادا مالية و خبايا استراتيجية قد تكون عاملا حاسما في تحديد مصيرها، و بالتالي فالفرضية الثانية صحيحة.

توصيات و مقترحات:

لمضاعفة آليات الوقاية و ضمان الأمان في المعاملات التجارية الالكترونية لابد من تتبع بعض هذه التوصيات:

- الاشتراك في شبكات الحماية العالمية عالية المستوى مثل (Kaspersky Security Network)
- استخدام أنظمة التشغيل المحمية مثل Linux.
- استخدام مضادات الفيروسات مع ضبط إعداداتها و تحيينها قدر المستطاع.
- الحرص على استخدام جهاز كمبيوتر آمن.
- التأكد من سمعة المتجر الذى نشترى منهوتتبع عملية الشراء.
- يكون التسوق أكثر أمنا من الكمبيوتر وليس من الهاتف الذكي.
- الاحتياط من الباعة الخاصين والتأكد من سمعة الموقع.
- تأمين الدفع ببطاقات الائتمان وتجنب البريد الإلكتروني الاحتيالي.

المراجع:

1د.أمال محمد محمد عوض، "دور آليات الحوكمة في تعزيز حوكمة تكنولوجيا المعلومات وضبط مخاطر الأنشطة الالكترونية للمنشآت"مجلة الدراسات المالية و التجارية، كلية التجارة، جامعة بني سويف، العدد الأول،2008.

2د.نجلاء إبراهيم يحي عبد الرحمن، "دور حوكمة تكنولوجيا المعلومات في ضبط مخاطر المنشأة في القطاع المصرفي السعودي"، ورقة عمل مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، عدد خاص، الجزء الأول، السنة السابعة عشر، أكتوبر2013، ص222.

3د.نجلاء إبراهيم يحي عبد الرحمن، مرجع سبق ذكره، ص 223.

4د.نجلاء إبراهيم يحي عبد الرحمن، مرجع سبق ذكره، ص 225.

5http://www.mohamah.net/answer/31275ورقة-بحثية-متميزة-حول-حوكمة-تقنية-المعلومات

03/01/2016

6https://ar-ar.facebook.com/acgroup.eg/posts/687759694653800 03/01/2016

7 دوج جيرلاش," الاستثمار عبر الانترنت ", ترجمة تيب توب لخدمات التعريب و الترجمة, دار الفاروق للنشر و التوزيع, مصر 2001 ص 279.

8 عبد الفتاح بيومي حجاز، " التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر و الانترنت"، الطبعة الاولى دار الفكر الجامعي ،الاسكندرية ، مصر ، 2006 ، ص 270.

9https://mustafasadiq0.wordpress.com/2014/09/30/التشفير-وانواعه/ 04/01/2016

10 نضال اسماعيل برهم " احكام التجارة الالكترونية " دار الثقافة للنشر و التوزيع، الأردن، 2005، ص 170.

11 عبد الفتاح بيومي حجاز ، " التجارة الالكترونية العربية ،الكتاب الاول : شرح قانون المبادلات و التجارة الالكتروني التونسي "، دار الفكر الجامعي، الاسكندرية ، مصر ،2004، ص93.

12http://www.q8control.com/_____11.htm05/01/2016

13 عبد الفتاح بيومي حجاز ، " التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر و الانترنت "،مرجع سبق ذكره، ص249.

14https://om77.net/forums/thread/434475--ما-هو-مفهوم-الشهادات-الرقمية-؟-جديد-العلم-والمعرفة/?s=d08597561b411aa637af44b073855f5a14605eb7 06/01/2016

15 احمد محمد غنيم، " الادارة الالكترونية، افاق الحاضر و تطلعات المستقبل"، المكتبة المصرية، المنصورة، مصر، 2004، ص 327.

16http://www.lahaonline.com/articles/view/41544.html09/01/2016.

17http://www.alriyadh.com/159573 10/01/2016.

18 يوسف احمد ابو فارة، " التسويق الالكتروني – عناصر المزيج التسويقي "،الطبعة الثانية، دار وائل للنشر، القدس فلسطين،2007،ص369.

19http://www.ee.washington.edu/research/nsl/students/alomair/LB-Arabic/arabic/is-dictionary/Secure-Socket-Layer-and-Transport-Layer-Security.html15/01/2016.

20www.ecommerceyechnologie.org21/01/2016.

21 احمد محمد غنيم، " الادارة الالكترونية، افاق الحاضر و تطلعات المستقبل"، المكتبة المصرية، المنصورة، مصر، 2004، ص ص 329-330.

22www.carjj.org/sites/default/files/semcybersecbeirut.pps27/04/2016.

[23]Mohamed Cherif BELMIHOUB, Rapport sur les innovations dans l'administration et la gouvernance dans les pays méditerranéens : Cas de l'Algérie, Avril 2004, P 20.

[24]علي العيادي، القطاع الخاص يدفع حوكمة الشركات في الجزائر، نشرة دورية للشرق الأوسط وشمال افريقيا، مركز المشروعات الدولية الخاصة، العدد 21، 2011.

[25]صبايحي نوال، ورقة بحثية بعنوان "واقع الحوكمة في دول مختارة–مع التركيز على التجربة الجزائرية"، المؤتمر الدولي الثامن حول :دور الحوكمة في تفعيل أداء لمؤسسات والاقتصاديات، ص 11.

[26]http://www.alwahatech.net/vb/showthread.php?t=2587827/04/2016.

[27]الجريدة الرسمية للجمهورية الجزائرية العدد 06، المؤرخة في 10 فبراير 2015، ص 06-16.

[28]www.carjj.org/sites/default/files/semcybersecbeirut.pps27/04/2016.

29http://info.worldbank.org/governance/wgi/index.aspx#home27/04/2016.