بسم الله الرحمن الرحيم

مخاطر العمليات المصرفية التي تتم من خلال القنوات الالكترونية

مجلة البنوك، العدد الثاني، المجلد الثالث والعشرون، اذار ٢٠٠٤، الاردن

أ د نعيم دهمش
رئيس قسم المحاسبة والتمويل
كلية الدراسات الإدارية والمالية العليا
جامعة عمان العربية للدراسات العليا

و

د ظاهر شاهر القشي
قسم المحاسبة
كلية الاقتصاد والعلوم الإدارية
جامعة اربد الأهلية

لقد احدث عصر العولمة وتقنية الاتصالات الحديثة المتمثلة بشبكة الانترنيت نقل نوعية في التعامل التجاري، حيث أزالت هذه التقنيات الحدود الاقتصادية بين الدول، ولما لهذه التقنيات من اثر كبير في تمكين الشركات من تحقيق إيرادات وأرباح كانت اقرب إلى الخيال بالماضي فقد بدأت الشركات بشتى أشكالها تسعى إلى الخوض في تلك التقنيات بشكل عام وبتقنية التجارة الإلكترونية بشكل خاص لتحقيق المكاسب الخيالية والسعي إلى المنافسة واكتساح الأسواق العالمية.

لقد كانت البنوك من أولى القطاعات التي تنبهت لأهمية هذه التقنيات الحديثة وسعت بشتى الطرق والوسائل إلى تبنيها وتداول الأعمال البنكية المتعددة من خلالها، وأيقنت كذلك أن تلك التقنيات الحديثة ستحدث تغييراً شاملاً على البيئة البنكية، وأخذت تؤهل نفسها والعاملين ببيئتها بشكل يمكنهم من مجاراة هذه البيئة الفريدة من نوعها.

وعلى سبيل المثال لا الحصر فقد عقد اتحاد البنوك الكندية Canadian Bankers Association's ممثلا للصناعة البنكية الكندية، وبالتعاون مع غرفة التجارة الكندية Canadian Chamber of Commerce، و معهد المحاسبيين القانونيين الكندي Canadian Institute of Chartered Accountants، والصناعة الكندية Canadian Industry من ٢٠٠٠/٥/٤ ولغاية ٢٠٠١/٦/٢١ ستة وسبعون مؤتمرا هدفت إلى تأهيل مؤسسات الأعمال بشكل يمكنها من الخوض بعالم التجارة الإلكترونية، وقد بلغ عدد المشاركين في تلك المؤتمرات ٨٠٠٠ مشارك. وقد تم تزويد جميع المشاركين بتلك المؤتمرات بجميع المعلومات الضرورية التي ركزت على إظهار أهمية التجارة عبر شبكة الانترنيت، والفرص المتوفرة عبر التعامل من خلال الشبكة العالمية، والكيفية التي يمكن من خلالها تحقيق نتائج باهرة عبر هذا النوع الجديد من التعاملات، والكيفية التي تمكن المشاركين من تأمين الحماية الضرورية لأنظمتهم المتعاملة مع شبكة الانترنيت، وتم اطلاعهم كذلك على جميع القوانين التي تساهم في توفير الحماية وتأمين العمليات والية الاحتساب الضريبي.

رغم الفوائد والإيجابيات الكثيرة التي رافقت هذه التقنيات التكنولوجية الحديثة، إلا انه رافقها سلبيات كثيرة بدأت تهدد وجودها إن لم يتم السيطرة عليها، وعلى رأس هذه السلبيات الجرائم التي ترتكب من خلالها، كجرائم الحاسوب بشكل عام وجرائم شبكة الانترنيت بشكل خاص، فلقد اصبح العالم يفيق كل يوم على واقع جريمة جديدة ترتكب من خلال هذه التقنيات الحديثة، وباتت هذه الجرائم تهدد اقتصاد الدول بشكل خطير جدا، ومن الملاحظ بأن تلك الجرائم تتزايد بشكل متسارع يجاري ويوازي التسارع التكنولوجي، وللأسف أصبحت فناً من الفنون له قواعده وقوانينه الخاصة.

ووفقا لما جاء في موقع www.e-commercealert.com وحسب ما جاء به تقرير إحدى الاستطلاعات بأنه وخلال عام ٢٠٠١ ما يقارب ١٢% من أنظمة الشركات المتعاملة عبر شبكة الإنترنت تعرضت لاختراقات كانت غالبيتها من البنوك حيث احتلت ما نسبته ٢٧% من مجمل الشركات التي تم اختراقها.

وقد اظهر التقرير بان أسباب الاختراقات تعددت، بحيث أن ٣٠% منهـا بسـبب فيروسـات هاجمت الأنظمة، و١٩% بسبب قراصنة الانترنيت ونجاحهم بالحصول على معلومات فائقة السـرية واستغلالها بسرقات مالية، و١٩% بسبب أخطاء بشرية، و٧% بسبب حدوث أعطال أو خلل ببرامج الأنظمة، و٢٥% لأسباب أخرى متفرقة.

ويمكن تصنيف جرائم هذه التقنية الحديثة ضمن فئتين رئيسيتين: ١- الهجـوم علـى مواقـع الشبكة بفيروسات معروفة وغير معروفة وإيقاع أضرار متعددة الأشكال والنتائج بأنظمة أصحاب تلك المواقع و٢- اختراق أنظمة الشركات عن طريق مواقعها الإلكترونية عبر شبكة الانترنيت والحصول منها على معلومات سرية خاصة بعملائها لاستغلالها بالجرائم المالية.

فقد ذكرت صحيفة ناشيونال بوست National Post في ٢٠٠٣/٢/١٩ وضمن مقاله معنونـة (قد استطاع قراصنة الانترنيت إلى الوصول إلى الملايين من بطاقات الاعتماد) بأن أحد القراصـنة استطاع اختراق قاعدة بيانات إحدى الشركات التي تعمل على إتمام تبادل العمليـات بـين التجـار (كوسيط) واستطاع أن يصل إلى معلومات بطاقات الاعتمـاد وأرقـام حسـابات عمـلاء الشـركة الإلكترونية. ووفقا لتصريحات هيئة بطاقات الاعتماد الدولية MasterCard International بأنه وبسبب ذلك الاختراق تأثر أكثر من ثمانية مليون حساب، منها ٣,٤ مليون حساب تخص حسابات بطاقـات الفيزا، و ٢,٢ مليون حساب تخص بطاقات الاعتماد.

وحسب تصريحات ريك بروهيد Rick Broahead (كاتب ومحلـل تكنولـوجي) بـأن ذلـك الاختراق يعد من اكبر الاختراقات التي اطلع عليها. وقد رفض المتحدث باسم هيئة بطاقات الاعتماد الدولية إعطاء أية تفاصيل عن الآلية التي تم الاختراق بواسطتها والكيفية التي تأثرت بها الحسـابات نتيجة ذلك الاختراق.

وقد قال السيد كيفين واسلين Kevin Wasslen (مدير إدارة المخاطر في هيئة بطاقات الاعتماد الدولية) بأننا لا نستطيع الجزم فيما إذا كانت المعلومات التي وصل إليها المخترق ستستخدم بأسلوب تلاعب أو غش أو خداع، من منطلق بأن بعض قراصنة الانترنيت يخترقوا أنظمة الشركات لغايـات التحدي لا اكثر ودون تبييت النية لاستخدام المعلومات التي يحصلون عليها لتحقيـق غايـات غيـر شرعية.

من الملاحظ بأن الشركات التي تصدر مثل هذا النوع من بطاقات الاعتماد التي تستخدم عبـر شبكة الانترنيت تحمي زبائنها وتمنحهم ضمانات أكيدة لتعويضهم عن أي خسائر تنتج من الاسـتخدام غير المصرح له لبطاقاتهم من قبل الغير. ومن الملاحظ كذلك بأن اغلب الشركات التي يتم اختراقها لا تعترف بحصول عملية الاختراق، وفي الحالة التي نتداولها لم تستطع الشركة التغاضي عن عملية الاختراق حيث أن عملائها هم الذين فضحوا الأمر للعموم، وقد اكتفت هيئة بطاقات الاعتماد الدولية بالقول بأنها كانت على علم بعملية الاختراق بمدة شهر واحدة من خروجها للعلن وبأنها لم تستطع أن تحدد إن كان الاختراق قد تم داخليا من الولايات المتحدة أم خارجيا.

مثل هذه القضية تطرح تساؤل مهم جدا، هل بالإمكان حماية الأنظمة المرتبطة بشبكة الانترنيت بشكل كامل؟ الإجابة بالطبع ستكون لا، فأي شخص يود اختراق أي نظام سيتمكن من ذلك عاجلا أم آجلا وخصوصا إن كان مؤهلا تكنولوجيا، فكل نظام ولا بد من وجود نقاط ضعف فيه يستطيع الغير استغلالها إن وجدها، ولاكن ما تستطيع الشركات عمله والتركيز عليه بالوقت الحاضر الاستمرار في البحث عن وسائل وتطوير أنظمة حماية ومواكبة كل جديد لتقليل الفرص أمام المخترق بالوصول إلى نظامها والحد من الخسائر التي قد يسببها.

ونستطيع أن نشبه الحل، كالقضية الأزلية بين القط والفأر أو بين الشرطي والمجرم، فمـا دام الشرطي يطارد المجرم تبقى السرقات متدنية ولكن لم ولن تنتهي.

وكمحاولة جدية للحد من الجرائم التي ترتكب عبر شبكة الانترنيت وتخفيف أضرارها، بدأت بعض الحكومات بالتوجه نحو سن قوانين وتخصيص جهات أمنية خاصة مؤهله تكنولوجيا للتعامل مع مثل هذا النوع من الجرائم، والتعاون مع الجهات المؤهلة تكنولوجيا لإيجاد حلول تحد من الاختراقات، وخير مثال على ذلك الحكومة الأمريكية، حيث أنشئت قسم خاص ضمن مكتب المباحث الاتحادي الأمريكي FBI أسمته IC3 (Internet Crime Complaint Center) مركز بلاغات جرائم الانترنيت. ووفقا ما جاء على موقع أل FBI (www.fbi.gov) فان هذا المركز يتألف من ٦٢ شخص عبارة عن وكلاء مباحث ومحللين، وعلماء حاسوب، وأخصائيين في تكنولوجيا المعلومات، ويتلقى المركز ما يقارب ١٢٠,٠٠٠ شكوى سنويا بخصوص اختراقات تحدث عبر شبكة الانترنيت، ومن ثم يقوم بتحليلها ومحاولة ضبط المخالفين وتقديمهم إلى القضاء، والعمل على إيجاد حلول ناجعة مستقبلا للحد من أي اختراقات جديدة قد تحدث.

ومن أشكال تعاون مكتب التحقيقات أل FBI ما جاء في التقرير المنشور في موقع Security Wire Digest في ٢٠٠٣/٦/٢ بأن معهد أمن الحاسوب Computer security Institute وبالتعاون مع مكتب المباحث الاتحادي الأمريكي FBI قاما باستطلاع أراء ٥٣٠ شركة أمريكية من الذين تعرضت أنظمتهم إلى اختراقات عبر شبكة الانترنيت، ووجدوا بأنه ورغم أن مستوى الاختراقات لا يزال عالي جدا وتصاعد بشكل ملحوظ منذ عام ٢٠٠١ إلا أن خسائر تلك الشركات المالية الناتجة عن عمليات الاختراقات انخفضت بما يقارب أل ٥٠%، فلقد انخفضت خسائر تلك الشركات البالغة في عام ٢٠٠١ ما يقارب أل ٤٥٥ مليون دولار سنويا لتصبح حاليا ما يقارب ٢٠١ مليون دولار سنويا.

ويتابع التقرير قوله بان بأن ٩٢% من الشركات عينة الاستطلاع يقرون بأنه وبالرغم من جميع الإجراءات الاحترازية التي يتخذونها، إلا أن عمليات اختراق أنظمتهم لا تزال جارية خلال العام، وكل ما استطاعوا فعله هو محاولة الحد من الخسائر التي يتكبدوها، والتي أحيانا يتمكنوا من حسرها في خسائر غير مالية تتمثل بفقدان أنظمتهم بعض المعلومات الخاصة، وتقر ٤٥% من الشركات بأن اغلب الاختراقات التي يتعرضوا لها تكون نتيجة تواطأ داخلي من بعض أفراد الإدارة، وأن ٧٨% من عمليات الاختراقات تتم عبر وسائط شبكة الانترنيت.

يذكر أحد تقارير أل FBI والمعنون (أن البنوك ابعد ما تكون عن تمكنها من توفير الحماية اللازمة لأنظمتها من قراصنة الانترنيت)، بأن البنوك ورغم استمرارها ببذل كل الجهود نحو دفع عملائها نحو التعامل معها عبر شبكة الانترنيت بشكل متزايد غير مسبوق، إلا أنها تبذل جهد اقل في تأمين أنظمتها وحمايتها من اختراقات قراصنة الانترنيت، والدليل على ذلك بأنه ورغم وجود أنظمة حماية لديها يفترض بها أن تحمي تعاملات عملائها الإلكترونية إلا انه ولغاية ألان لا تزال الاختراقات جارية لتلك التعاملات، فقد تلقى مكتب التحقيقات خلال عام ٢٠٠٠ ١٧٠٠٠ بلاغ عن اختراقات تمت في تلك الفترة تجاوزت خسائرها ما يقدر ب المليار ونصف المليار. ويذكر تقرير آخر صدر في مطلع هذا العام بأنه وفي حالة حدوث عمليات اختراق ناجحة للنظام البنكي والمالي في الولايات المتحدة الأمريكية فانه سيشل الحكومة تماما في غضون ثلاثة أيام فقط، ويظهر التقرير بعض المؤسسات المالية في العالم التي تعرضت لاختراقات عبر شبكة الانترنيت، والتي تضمنت مؤسستين ماليتين رائدتين وهما Citibank و Guardian Insurance ويذكر أل FBI أن المشكلة الرئيسية في حدوث الاختراقات لتلك المؤسسات المالية وعلى رأسها البنوك هو عدم توظيفها المصادر التكنولوجية الكافية لتأمين الحماية والاكتفاء بطاقم تكنولوجي ضئيل نسبيا.

لقد تبهت بعض الجهات المحاسبية المتخصصة للقصور التكنولوجي الموجود لدى الكثير من الشركات المتعاملة بالتجارة الإلكترونية عبر شبكة الانترنيت، وبدأت السعي الجاد لإيجاد حلول جذرية لمعالجة ذلك القصور، ومن افضل الأمثلة على تلك الحلول، المشروع المشترك بين معهد

المحاسبين القانونيين الأمريكي (AICPA)، ومعهد المحاسبين القانونيين الكندي (CICA)، والذي بدأ العمل به وتطويره في نهاية التسعينات، وتم إطلاقه أخيرا في ٢٠٠٢/٧/١.

المشروع هو عبارة عن خدمة تدقيق إلكترونية جديدة أطلق عليها اسم موثوقية الموقع Webtrust، وهي عبارة عن منح الشركة الراغبة بالحصول على هذه الخدمة الجديدة ختماً إلكترونيا يوضع على صفحة موقعها بحيث يبين للمتعامل معها بأن موقعها يتم تدقيقه من قبل أحد منتسبي المعهدين.

يشرح هذا المشروع المشترك لجميع الشركات المتعاملة بالتجارة الإلكترونية، والراغبة بتوكيل مدقق خارجي من هذه الهيئات المحاسبية المشاركة بالمشروع ، الآلية والإجراءات التي سيقوم بها المدقق لضمان حماية نظامها المحاسبي من المخاطر المرافقة للتعامل بالتجارة الإلكترونية ، وبالتالي إضفاء الأمان والتوكيدية والموثوقية لجميع مدخلات ومخرجات النظام.

تتكون أجزاء هذا المشروع من التالي:

١ شرح مفصل عن ماهية التجارة الإلكترونية.
٢ ماهية المخاطر المرافقة للتعامل بالتجارة الإلكترونية عبر الانترنيت.
٣ الأثر العالمي لموضوع الخصوصية.
٤ سلبية العمليات المحاسبية في غياب التوثيق المستندي.
٥ آلية حماية المعلومات وتعقيداتها.
٦ شرح للمبادئ الكفيلة بحماية صفحات التصفح عبر الانترنيت (Web Trust Principles).

ويمكن تلخيص المبادئ بالتالي:

- الحماية (Security) ، وينص على أن النظام محمي من الاختراقات غير المصرح بها.
- جاهزية النظام (Availability) ، وينص على أن النظام جاهز للعمل وفقا للسياسات الموضوعة.
- سلامة وتكامل الإجراءات (Processing Integrity) ، وينص على انه قد تم التأكد من أن جميع الإجراءات قد تم تجهيزها وأنها توفر معلومات دقيقة ووقتية ومصرح بها.
- الخصوصية على الشبكة (Online Privacy) ، وتنص على أن الاستخدام والإفصاح عن جميع المعلومات التي تم الحصول عليها عبر التعامل بالتجارة الإلكترونية من خلال شبكة الانترنيت ، يتماشى مع سياسات الشركة الموضوعة لتأمين الخصوصية للمتعاملين معها.
- السرية (Confidentiality) ، وتنص على أن سرية جميع المعلومات ، تتماشى مع سياسات الشركة الموضوعة لتأمين سرية المعلومات.

والسؤال الذي يدور بالأذهان، إذا كان هذا حال شركات وبنوك العالم المتقدم والتي اكتسحت السوق عبر شبكة الانترنيت، فما هو حال شركات وبنوك العالم النامي بشكل عام، وشركات وبنوك الأردن بشكل خاص؟ وخصوصا أنها لا تزال على عتبات التقنيات الحديثة. هل هي جاهزة للخوض في هذه التقنيات الحديثة؟ ومذا اعدت من اجراءات تكفل حمياتها من المخاطر المرافقة لها؟