مهددات شبكات البنوك

من خلال منظور كل من (بنك السودان المركزي، بنك الخرطوم، بنك ام درمان الوطني)

محمود إبراهيم حمد

كلية مروي التقنية، قسم أنظمة الحاسوب، مروى، السودان

محمود علي أحمد

جامعة الخرطوم , كلية العلوم الرياضية، الخرطوم، السودان

بازرعة إمام برى

جامعة الخرطوم، كلية العلوم الرياضية، الخرطوم، السودان

المستخلص :-

نبعت اهمية هذة الورقة من ضرورة التعرف على مخاطر الشبكات المصرفية وذلك من خلال إعداد استبيان وُزِّع على البنوك المختارة وفروعها وهي بنك أم درمان الوطني، بنك الخرطوم، بنك السودان، وذلك لمعرفة ماهى الأصول التى نحتاج لحمايتها فى الشبكة ومن أى المصادر يجب حماية هذه الأصول وماهى نوعية مهاجمي نظم الشبكات ومن أي الطرق يمكن أن يتم اختراق الشبكات.

الكلمات المفتاحية :

البنوك الإلكترونية، مخاطر الشبكات، تامين الشبكات

The Importance of this paper comes from the necessary of knowing the risks which faces the net work banking systems, A survey has been prepared and distributed to selected banks, Such as Omdurman National Bank, Bank of Khartoum, and Bank of Sudan and its branches .In order to know the assets which need protection in the network and from sources has to protect the same, and the Hackers of network system and ways of networks which may attacked

Electronic Banking, network risks, security network

:Key words

يسمح هذا الموقع بتبادل الإتصال بين البنك وزبائنه كالبريد الإلكتروني وتعبئه طلباته علي الخط او تعديل حساباته.

٣-٣ الموقع التبادلي Transactional :

ويستطيع البنك بواسطة هذا الموقع أن يقوم بكل خدماته وأنشطته في ظل بيئة الكترونية، فيمكن للعميل الوصول الي حساباته وإدارتها وإجراء الدفعات النقدية والوفاء بقيمة الفواتير وإجراء كافة الخدمات الإستعلامية وإجراء التحويلات بين فرع البنك وأى بنك اخر.

٤-الخدمات المصرفية عبر الإنترنت

هنالك عدد من الخدمات البنكية التي يتم تقديمها عبر الأنترنت كالإستعلام عن أرصدة او تحويل بين حسابات او تسديد فواتير او غيرها .

وقد ارتقت هذه الخدمات بالعملية المصرفية حيث تتيح التوسع فى الخدمات البنكية في ظل الانترنت وشبكاته وتسهم فى خلق فرص تنافسية كبيرة ، كما تتيح تقديم خدمات مصرفية مبتكرة يمكن ان تنافس بها في سوق العمل كما يمكن توفير تكاليف التشغيل الخاصة بالبنك والمؤسسات المالية عن طريقها.

كل ذلك يساعد في تحسين كفاءة المدفوعات والأنظمة البنكية ويسهم في خفض تكلفة الإجراءات الخاصة بعملائها علي الصعيد المحلي والعالمي وترفع كفاءة العمل داخل البنك .

الى ذلك تقوم الخدمات المصرفيه عبر الانترنت بتوفير عدد من القنوات وطرق الإتصال بالبنك للزبائن الذين كانوا يعانون من محدودية هذه الأنظمة بالسابق[٥] .

كل هذه الخدمات التي يتيحها استخدام الأنترنت للمصارف المالية قد تشتمل علي مخاطر عديدة ليست فقط للمصارف بل لمعظم القطاعات المهنية اذ تعانى جميع هذه القطاعات المهنية لخطر الهجوم عليها(٦) وهوكما موضح فى الجدول ١

جدول١: القطاعات المهنية التى تعانى من الهجوم والنسب المئوية

القطاعات المهنية المهاجمة	النسبة المئوية
المالية والتأمين	١٩,٤٣٪
التصنيع	١٠,٦٪
الخدمات	٢٤,٣٢٪
المتاجر	١٥,٦٩٪
الاغذية والادوية	٥,١٦٪
الحكومة	٧,٥٦٪
تكنلوجيا المعلومات	٤,٢٦٪
العناية بالصحة	٢,٨٦٪
الاستشارات	٢,٥٩٪
الموصلات	١,٢٦٪
التعليم	١,١٣٪
الاتصالات عن بعد	١,٠٩٪
الترفية	٠,٦٤٪
الخدمات القانونية	٠,٠١٪

وقد أكدت تقارير علمية أن العام ٢٠٠٧ شهد أعلى نسبة للإختراق في تاريخ الاتصالات اذ تم تسجيل ١٦٢ مليون شكوى من حالات سرقة البيانات الشخصية والحسابات المالية وبطاقات الإعتماد ويتوقع الخبراء زيادة هذة النسبة فى الاعوام المقبلة [٧] فقد تستغل تكنلوجيا المعلومات وتقنياتها للإستيلاء على الأموال باجراء تحويلات غير شرعية فقد كانت البنوك عرضة لحالات الإختلاس والتلاعب بحسابات العملاء [٨] وتختلف اسباب الإختراق من شخص لآخر فمعظم الإختراقات التى تحدث هدفها الأنظمة المالية كأنظمة الدفع فى البنوك , والحصول على ارقام الإئتمان والمعلومات البنكية [٩] لذلك يجب إجراء التحويطات الازمة لتفادي هذه المخاطر, وتطوير اجراءات الحماية لتواكب تطور الاختراقات .

الإسلامى بالخرطوم ندوة بعنوان (تسويق الخدمات المصرفية الإلكترونى) ومن خلال الندوة قدمت ورقة عمل حول الاطار القانونى للصرافة الإلكترونية واشارت الورقة الى انواع الخدمات المصرفية التى تشمل الصرفات الآلية , الهاتف المصرفى , الهاتف الجوال والصرافة عبر شبكة الانترنت كما اوضحت الورقة ان هنالك عددا من التحديات التى تعترض إثبات العمليات المصرفية منها الإثبات والتعدى على الاموال والمعلومات فى بيئة العمل المصرفى الإلكترونى مما دفع بصدور مشروع قانون مكافحة جرائم المعلومات لسنة ٢٠٠٦ [١٤].

٧- التشريعات والقوانين فى البيئة الإلكترونية

تعتبر السويد اول دولة سنت تشريعات خاصة بالإنترنت حين اصدرت قانون البيانات السويدى عام ١٩٧٣ واتبعتها بقية الدول وجاءت الولايات المتحدة الامريكية كثانى دولة تسن تشريع فى هذا الصدد حيث شرعت قانون خاص بحماية الحاسب الآلى عام(١٩٧٦) وجات بريطانيا فى المرتبة الثالثة فقد اقرت قانون مكافحة التزوير والتزيف عام ١٩٨١ وتبعتها الدنمارك , فرنسا , هولندا , اليابان , المجر , وبولندا , وعلى المستوى العربى جات تشريعات قوانين تدين مرتكبى تلك الجرائم , حديثا , اما فى السودان فقد اصدرت وزارة العدل امرا بتأسيس نيابة متخصصة فى التحقيق فى جرائم المعلومات وتقديم مرتكبيها للمحاكمة, وكانت إحدى أهداف قانون المعاملات الإلكترونية في السودان لسنة ٢٠٠٧ هو توفير الحماية الجنائية للتبادل الإلكتروني للبيانات ومنع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الإلكترونية (١٥)، وتعتبر المرة الاولى فى السودان التى تحاكم فيها هذه الجرائم اتساقا مع التوجه العالمى لمكافحة هذه الجرائم التى تستخدم فى عمليات الارهاب وغسل الاموال والجريمه العابرة , ويحاكم القانون الذى أجيز فى عام ٢٠٠٧ على دخول المواقع وانظمة المعلومات المملوكة للغير والاطلاع او النسخ او الغاء البيانات او المعلومات او افشائها او تدميرها او إعادة نشرها دون وجه حق او تغيير مضامين الموقع او عنوانه كما تحاكم الموظفين الذين يدخلون دون اذن الى نظم المعلومات الخاصة بالجهة التى يعملون فيها او تسهيل ذلك للغير او تدمير البرامج او اعاقة او تشويه الوصول للخدمة او استخدام شبكة المعلومات او اجهزة الحاسوب للتهديد او الابتزاز او انتحال الشخصية او استعمال الاسماء الكاذبة بغرض الاستيلاء على اموال او سندات للغير او الحصول على معلومات او بيانات تمس الامن القومى او الاقتصاد . وتتراوح عقوبات السجن مابين سنتين وعشر سنوات بحسب نوع وخطورة الجريمة [١٦].

٨- دراسة مهددات شبكات البنوك

تناولت الدراسة تحليل مهددات شبكات البنوك من خلال منظور كل من بنك السودان المركزى وبنك الخرطوم وبنك أمدرمان الوطنى، وهى تعتبر من أكبر وأهم المصارف المالية بالبلاد من حيث عدد العملاء والفروع، كما أنها من اشهرالمصارف الوطنية الموجودة بالبلاد.

تم تصميم وتوزيع استبيان اولى لتعرف على مهددات المصارف عموماً مكون من ٢٠ شخص من زوى الخبرة ,وبناءً على ماتحصلنا علية من مخاطر ومهددات قمنا بتصميم استبيان نهائى تضمنت العديد من المحاور، ومن خلال تحليل الاستبيان بواسطة برنامج (SPSS)) تم التوصل الى عدد من النتائج.

وشملت الدراسة ١٧٩ موظف شكلوا عينة عشوائية من حجم العينة الكلى البالغ ٨٧٤ موظف، تم تحديد حجم العينة وفقاً ل قانون استخدام تحديد حجم العينة فى الدراسات الوصفية لوليام كوكرن من خلال القانون التالى :

$$N = (Z^2_{\alpha/2}\ P(1-P)) / D^2$$

P: proportion of employee (good)

P = 50% = 0.5

1-p = 50% =0.5

$Z_{\alpha/2}$: critical value (توجد فى جدول التوزيع الطبيعى)

α=significance level (مستوى الدلالة)

٨-١ الأصول التى تحتاج لحمايتها فى الشبكة

يجب علينا في تحليل المخاطر ان نحدد الأصول والموارد التي تحتاج للحماية من الإختراقات وقد هدف الباحث من الإستبيان إلى معرفة الأصول التي تحتاج للحماية في الشبكة (المادية، البرمجية) كأجهزة الحاسوب وأجهزة الإدخال والإخراج وأجهزة التحكم والكوابل المستخدمة في الشبكة وغيرها ، والبرمجية كبرامج التشغيل والبرامج التطبيقية والأنظمة المستخدمة والبيانات المالية وقواعد البيانات وغيرها من أشكال البرامج الأخرى التي تحتاج للحماية. وقد تضمنت٠

الدراسة جملة من الافتراضات حول الأصول التى تحتاج للحماية فى الشبكة ،حسب ما يوضحها الجدول التالي :-

جدول(٣) يوضح الأصول التي تحتاج حماية في الشبكة

أصول الحماية	Count	Pct of Responses	Pct of cases
المكونات الصلبة	115	33.5	64.2
برامج الحاسوب	101	29.4	56.4
اجهزة التحكم	38	11.1	21.2
اجهزة المخرجات	49	14.3	27.4
الكابلات	40	11.7	22.3
Total responses	343	100.0	191.6

Missing cases:179 valid cases

أولاً الأصول المادية :- للأصول المادية عدد من الأشكال تشمل وحدات العمل ووحدات الخدمة والوحدات الطرفية وجميع المكونات المادية لأجهزة الحاسوب وأجهزة التخزين وأجهزة المراقبة والاجهزة الطرفية. وتعتبرالمصادرالمادية من أهم الأصول فإذا استطاع الشخص التحكم بهذه المصادر المادية يمكن إن يسيطر على كل نظام المعلومات كما يمكن أيضا إن يعبث في هذه الأجهزة وبالتالي يتوقف النظام عن العمل .

ويقصد بالأمن المادي هو التصدي للتهديدات التي تواجه الدخول الفعلي لسرقة الأجهزة أو سرقة الملفات والتحايل على الموظفين بالتنكر للوصول وذلك بعدد من الإجراءات التي تتخذها المؤسسة للحد من الدخول الغير مشروع منها فحص والتحقق من هويات الموظفين وذلك بالتحقق من بطاقات الدخول وغيرها من وسائل الحماية المادية .وعلى حسب عينة الدراسة جاءت المكونات المادية للأجهزة من اكثر الأصول التي تحتاج للحماية في الشبكة بتكرار ١١٥ وبنسبة ٦٤,٢٪ وهى تمثل اعلى نسبة من الاصول والموارد التى تحتاج للحماية .

ثانياً برامج الحاسب :- هي أحدى مكونات نظام المعلومات التي يجب حمايتها بصورة جيدة وذلك لما تحتويه البرامج من أهمية في عملية التشغيل والتحكم في أجهزة ومكونات الشبكة.

فهنالك عدة أنواع من برامج الحاسب كبرامج أنظمة التشغيل والبرامج التطبيقية

فيمكن إن يكون البرنامج اى شكل من إشكال البيانات والتي تلعب دورا في مجال عمل المؤسسة فيمكن أن تشمل بيانات مالية وسجلات قواعد البيانات للعملاء ,فمن أكثر المهددات التي تواجهه البرامج هجمات البرمجيات والأبواب الخلفية الديدان , أحصنة طروادة , القنابل المنطقية وتقدر الأضرار الناتجة من البرمجيات الخبيثة بين ١ إلى ٣ مليار دولار ,وتشمل هذه البرمجيات كل من الفيروسات وحصان طروادة والدودة الإلكترونية والقنابل المنطقية . وكل هذه البرمجيات تعتبر برامج تضر بالنظام وتؤدى إلى تدميره [١٧].

وعلى حسب عينة الدراسة جاءت برامج الحاسوب في المرتبة الثانية من أكثر الأصول التي تحتاج للحماية في الشبكة بتكرار بلغ ١٠١ بنسبة ٥٦,٤٪.

ثالثاً أجهزة المخرجات :- تعد أجهزة مخرجات نظام المعلومات كالطابعات والفاكسات من الأجهزة المكونة للنظام التي يجب حمايتها والتحكم في مخرجاتها لأن ما يطبع منها أو ما يخرج إذ استطاع المهاجم الحصول علي مخرجاته سيتعرف على كثير من المعلومات والبيانات والتي قد تكون في غاية الأهمية والسرية فمخرجات الحاسوب قد تتضمن معلومات سرية .

الاختراق عبر المخلفات التقنية يقصد به ان المهاجم يستطيع البحث عن اى شى فى مخلفات المؤسسة لإيجاد ما يساعده فى الهجوم على النظام كالأوراق ومخرجات الحاسوب الأقراص الصلبه بعد استبدالها وكل اجهزه التخزين التى يستطيع من خلالها معرفه كل مايحتويه النظام وما يساعده فى الاختراق كما يمكن معرفه ماتحتويه بعض الملاحظات المهمله التى تساعده على الاختراق .

وعلى حسب عينة الاختبارجاءت أجهزة المخرجات فى المرتبة الثالثة من حيث الأصول التي تحتاج حماية في الشبكة بنسبة ٢٧,٤٪ وبتكرار بلغ ٤٩ .

رابعاً وسائل نقل البيانات :- هنالك عدد من وسائل نقل البيانات عبر الشبكات منها اللاسلكية كالأقمار الصناعية وأشعة المايكرويف وموجات الراديو ويمكن إن يحدث خلل اثناء انتقال الإشارة من المصدر الى الهدف مما يتسبب في تغيير الإشارة .

اما النوع الآخر من وسائط النقل هى الوسائط السلكية مثل الكوابل وتعانى ايضاً هذه الوسائط من عدة مهددات منها الإلتقاط اللاسلكى ويقصد به توصيل سلك على الشبكة يستطيع المهاجم من خلاله التنصت على البيانات ومعرفة محتواها ويمكن تعديلها وسرقتها.

ويتوقف ذلك الخلل بعدد من العوامل كنوع الوسط المستخدم في النقل ومعدل سرعة

تدفق البيانات المنقولة والمسافة التي تبعد بين المرسل والمستقبل.

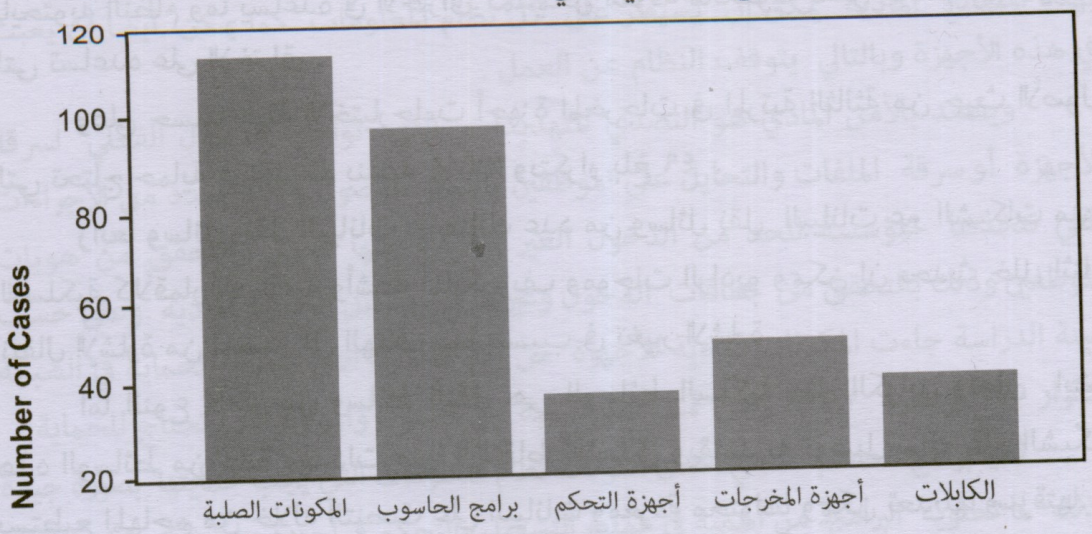
وقد وضعت عدة تدابير خاصة للحد من مشاكل وسائط النقل وذلك بتطبيق عدد من الإجراءات كوسائل للتحقق من سلامة الارسال والاستقبال .

وحسب عينة الدراسة جاءت حماية جميع الكابلات المستخدمة لنقل الصوت والبيانات الالكترونية بتكرار بلغ ٤٠ بنسبة ٢٢,٣٪ وهى نسبة ضعيفة مقارنة مع مكونات أجهزة الحاسوب وبرامجه.

خامساً أجهزة التحكم:- هنالك عدد من الأجهزة المستخدم في التحكم في تدفق الصوت والبيانات الإلكترونية كأجهزة موزعات الكيبلات ((Hub وهى عبارة عن أجهزة توصيل مركزية يمكن ان تكون أهداف للهجوم ، فمن السهل تخريب موزعات الكيبلات إذا كان المهاجم أو المخرب يملك وصولاً ماديا إليها اما المبدلات والجسور (Bridges And Switches) فانها تحتوي على جداول تطابقات العناوين (Media Access Controls (MAC ممايجعلها هدفاً محتملاً للهجوم, تحافظ الموجهات (Router) على مخابىء (ARP Address Resolution Protocol) وبما ان هذه الجداول تتيح للموجه إرسال وتوجيه الإتصالات بشكل مناسب على الشبكة ، فهى أيضاً تكون نقاط محتملة للهجوم (كما ايضاً .

بصورة عامة يعتمد بعض المهاجمين على السيطرة على أجهزة التحكم مثل أجهزة المودم وكروت الشبكة وأجهزة تكرار الإشارة للحصول على المعلومات المهمة .

جاء اختيار عينة الدراسة لاجهزة التحكم متدنية بتكرار بلغ ٣٨ بنسبة ٢١,٢٪ , وسيتم توضيح النتائج من خلال المدرج التكراري التالي :-



شكل(١) الأصول التي تحتاج حماية في الشبكة

٢-٨ غرض الهجوم على الشبكات

لكي نستطيع أن نحدد كيف نحمى نظم الشبكات بصورة جيدة يجب في البداية إن نتعرف على غرض الهجوم على شبكات المصارف.فمعظم الإختراقات والهجمات على الشبكات لا يتم اختراقها عن طريق الصدفة بل يتم التخطيط لها مسبقا. فهنالك عدد من الإغراض التي من اجلها يتم اختراق الشبكات وقد تطرقنا في هذه الدراسة التحليلية لبعض الأنواع الشائعة لإغراض الهجوم على الشبكات وهى كما موضحة فى الجدول التالى :-

جدول (٤) غرض الهجوم على الشبكات

غرض الهجوم على الشبكة	Count	Pct of Responses	Pct of cases
التعديل	71	20.3	40.1
السرقة	66	18.9	37.3
دمار البرامج	135	38.7	76.3
التجسس	77	22.1	43.5
Total responses	349	100.0	197.2

Missing cases:177 valid cases 2

أولاً دمار البرامج : يتم دمار البرامج بعدة صور كتدمير ملفات العملاء او تدمير برمجيات التطبيقات أو نظم التشغيل وذلك من خلال انتحال الشخصية اواستغلال نقاط الضعف اوقرصنه البرمجيات وهى نسخ او تعديل او محاكاه البرمجيات دون اذن او تخويل من منتج هذه البرمجيات .

وتمثل الفيروسات أكثر المهددات التي تتسبب في دمار برامج الحاسوب ويؤدى دمار البرامج لفقدانها وعدم اتاحيتها حيث ان عدم توفر المعلومة وقت الحاجة اليها يتسبب احيانا فى تكبد المصارف المعتمدة على هذه البرامج لخسائر طائلة .

ومن هنا تبرز أهمية اتاحية البرامج كعنصر رئيس فى مفهوم التأمين فقد جاء دمار البرامج أعلى نسبة من أغراض الهجوم على الشبكات بتكرار بلغ١٣٥ على حسب نسبة الدراسة وبنسبة ٧٦,٣٪.

ثانياً التجسس: يمكن تصنيف جواسيس الحاسب الى نوعين هواة ويتميز هولاء بأنهم يمتلكون خبرة بسيطة في مجال الاختراق, والنوع الآخر هم جواسيس محترفين وهم أكثر من الهواة بامتلاكهم خبرة تقنية في هذا المجال .

معظم مكونات نظم الحاسوب والشبكات تحتاج للحماية من خطر التجسس مثل البريد الالكتروني، كلمات المرور، الاتصالات المرئية والصوتية وغيرها. هنالك بعض التطبيقات للحد من خطر التجسس مثل كميرات المراقبة والتشفير وكلمات المرور وأنظمة الجدارن النارية وانظمة كشف الاقتحام .

وبشكل عام معظم المؤسسات تعانى حوادث فقدان البيانات وهذا يدل على قيام احد الاشخاص بالتجسس وسرقة تلك المعلومات وقد جاء التجسس فى المرتبة الثانية من اغراض الهجوم على الشبكات بتكرار ٧٧ وبنسبة بلغت ٤٣,٥٪ .

ثالثاً التعديل : المحافظة على حماية و تأمين البيانات من التعديل من أهم متطلبات التأمين، فيجب ان لايتم تغيير أو تحريف المعلومة إلا من قبل الأشخاص المصرح لهم، وتعتمد سلامة النظام على عنصرين أساسيين هما سلامة المعلومة وسلامة المصدر فسلامة المعلومة نعنى بها أن المعلومة لن تتغير بشكل غير ملائم سواء بالصدفة أو من قبل عمل متعمد .

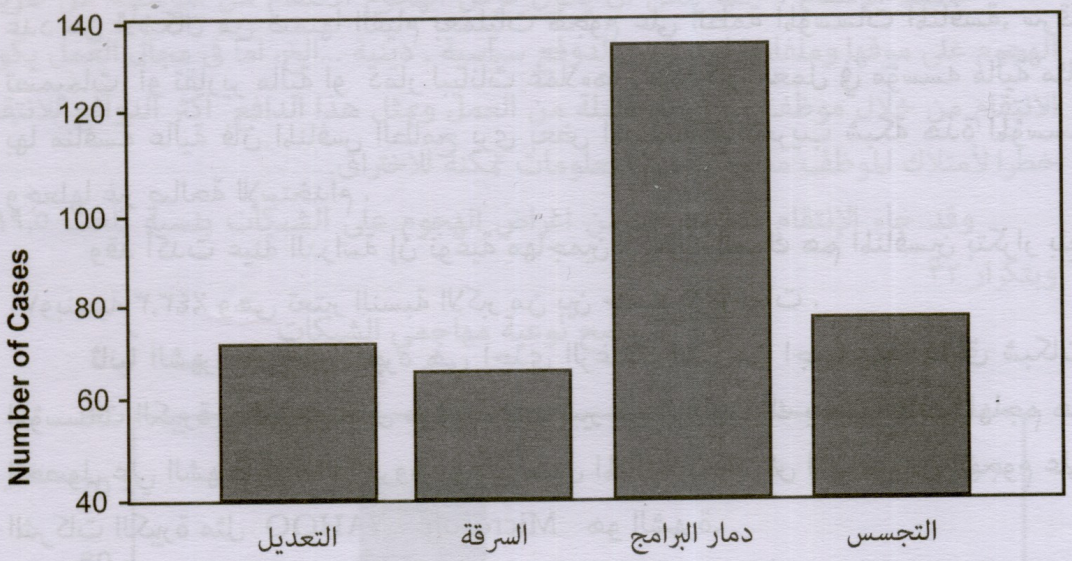
لذلك يجب التأكد في حالة الإرسال بأن البيانات التي تم استقبالها هي نفس البيانات التي تم إرسالها دون اى تعديل فيها .

فيمكن إن يحدث التعديل بإضافة بعض المتغيرات أو حذف بعض المحتوى أو تعديل في محتوى الرسالة او تحويلها.وتعتبر أرصدة العملاء من اهم المعلومات داخل البنوك فإذا استطاع المخترق الحصول على تلك البيانات يمكن إن يعدل في المبالغ لتصبح أضعاف المبالغ الأصلية .لذلك يجب الحماية ضد اى تعديل غير مرخص به لضمان سلامة المحتوى وهنالك عدد من الطرق للحفاظ على سلامة البيانات من التعديل منها على سبيل المثال التشفير وشبكاتVPN

وعلى حسب عينة الدراسة فقد جاء الغرض من الهجوم على الشبكة التعديل بتكرار بلغ ٧١ بنسبة بلغت ٤٠,١٪.

رابعاً السرقة:- تعد سرقة المعلومات من أهم أهدف الاختراقات للشبكة خصوصاً اذا كانت هذه الشبكة لمؤسسات مالية وتعتبرسرقة البيانات المالية من اكثر أنواع الاختراقات شيوعا، ويمكن ان تكون السرقة لأغراض اخرى غير المال كسرقة بعض الخرائط الرسومية والمخططات وغيرها .وعلى حسب إفراد عينة الدراسة جاء غرض الهجوم على الشبكة السرقة اقل افتراض بتكرار بلغ ٦٦ وبنسبة ٣٧,٣٪ .

شكل(٢) غرض الهجوم على الشبكات



٨-٣ نوعية مهاجمي الشبكة :-

لمعرفة الإخطارالتى تهدد الشبكات لابد ان نتعرف على مصدر هذا الهجوم وأنواع المهاجمين والدافع الذي أدى للهجوم، ويعتمد الهجوم على نوعية النظام المراد اختراقه وتعتبرالانظمة المصرفية والبنكية من أكثر الأنظمة التى يتم اختراقها من غيرها. ولمعرفة نوعية مهاجمين شبكات البنوك تم طرح عدد من الافتراضات على أفراد العينة، فكانت النتائج كمايلي:

جدول (٥) يوضح نوعية مهاجمي الشبكات

نوعية مهاجمي نظم شبكتك	Count	Pct of Responses	Pct of cases
الموظفون المحليون	45	18.5	27.4
المنافسون	71	29.2	43.3
الافراد الذين لديهم وجهات نظر	47	19.3	28.7
مختلفة	32	13.2	19.5
الافراد الذين يريدون الانتقام	48	19.8	29.3
الافراد الذين يرغبون فى شهرة	243	100.0	148.2

15 Missing cases:164 valid cases

أولاً التنافس :- أصبح التنافس كبير بين الشركات فى كل المجالات، وقد يأخذ التنافس عدد من الأشكال من ضمنها القيام بعمليات هجوم على انظمة المؤسسات المنافسة, سرقة تصميمات أو تقارير مالية او دمار لبيانات عملاءها , فإذا كان العمل في مؤسسه مالية مثلا بها منافسة عالية فأن المنافس الطامح يرى بعض المصلحة في تخريب شبكة هذة المؤسسة وجعلها غير صالحة للإستخدام .

وقد أكدت عينة الدراسة إن نوعية مهاجمين شبكات البنوك هم المنافسين بتكرار بلغ ٧١وبنسبة ٤٣,٣٪ وهى تعتبر النسبة الاكبر من بين جميع الافتراضات .

ثانياً الشهرة :- تعتبرالشهرة هي احدى الرغبات التى من اجلها يتم اختراق شبكات المؤسسات الكبيرة والتي يستقبل موقعها عدد كبير من الزوار لذلك يكون هدف المهاجم هو الحصول علي الشهرة وإرضاء الغرور , وعلى سبيل المثال كان الغرض الأساسى من الهجوم على الشركات الكبيرة مثل YAHOO, Microsoft هو الشهرة.

وعلى حسب أفراد عينة الدراسة كان الافراد الذين يرغبون فى الشهرة نتيجة لهجومهم على مواقع البنك في المرتبة الثانية بتكرار بلغت ٤٨ ونسبة بلغت ٢٩,٣٪.

ثالثاً وجهات النظر المختلفة: إذا كانت إحدى المؤسسات تعمل فى مجالات مثيرة للجدل سيكون هنالك وجهات نظر مختلفة على اعمالها , كمؤسسة ترعى عملية الإستنساخ البشري تكون عرضه للتهديدات من جهات تختلف معها في وجهات النظر ويكون التخريب بشكل متعمد كما يعتبر بعض الأشخاص المؤسسات المصرفية أنها مؤسسات ربوية وخصوصاً البنوك الغير اسلامية .

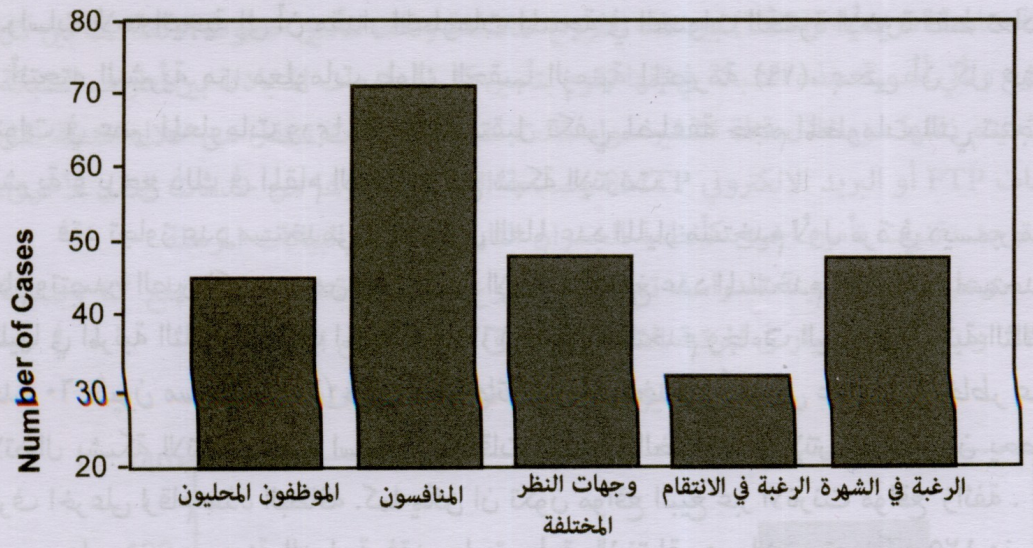
وقد اظهرت نتائج الدراسة إن نوعية مهاجمين البنك من الافراد الذين لديهم وجهات نظر او اهداف مختلفة في المرتبة الثالثة بتكرار بلغ ٤٧ ونسبة ٢٨,٧٪ .

رابعاً الموظفون المحليون: ويمثل الموظفون المحليون احدى مهددات الشبكات اذ لم يلتزم كل موظف بالاجراءات التأمنية داخل المؤسسة المعنية ,لذلك يجب علينا عدم الثقة الكلية بكل الموظفين المحليين، فيمكن مراقبتهم أثناء دوام العمل بوضع كميرات مراقبة لمراقبة وجودهم داخل المؤسسة وعمل كلمة مرور خاصة لكل جهاز من اجهزة البنك، فالإلتزام بهذة الاجراءات يقلل من المشاكل التى يسببها الموظفون، ومن خلال عينة الدراسة تبين ان الموظفين المحليين يمثلون نسبه ٢٧,٤ ٪ وتكرار ٤٥ من مهاجمى الشبكات وهذة النسبة تاتى فى المرتبة الرابعة .

خامساً الإنتقام :- كما يمكن ان يكون غرض الهجوم الانتقام من المؤسسة عن طريق الهجوم على موقها وملفاتها لعدد من الدوفع سياسية , دينية ...الخ، اما فى مجال العمل يكون الانتقام من خلال موظف سابق تم فصلة من العمل ويمثل هذا الدافع اكثر الدوافع للانتقام خطراً لأمتلاك الموظف مجموعة من المعلومات تمكنه للاختراق.

وقد جاء الإنتقام كأقل فرض من اغراض الهجوم على الشبكات بنسبة بلغت ١٩,٥٪ وبتكرار ٣٢

شكل(٣) يوضح نوعية مهاجمي الشبكات



٨-٤ من أى الطرق يمكن ان يتم اختراق الشبكات

أشارت الدراسات بأن معظم الاختراقات على نظم التأمين على الشبكات تتم من داخل المؤسسات فقد أظهرت الدراسات بأن حوالي ٨٠٪ من الإختراقات على الشبكات قام بها أفراد من داخنتقامل هذه المؤسسات أو عن طريق أفراد لديهم معلومات داخلية وبحسب تقديرات معهد أمن الحاسوب (CSI) فان تكاليف الهجوم من الداخل هو ٢,٧ مليون دولار للهجوم الواحد بينما لا يزيد معدل الهجوم الواحد القادم من الخارج عن ٧ ألف دولار (١٨) .

تم طرح مجموعة من الإفتراضات على أفراد العينة لمعرفة الطرق التى يتم خلالها الهجوم على شبكات البنوك فكانت النتائج كمايلي :

جدول (٦) يوضح طرق اختراق الشبكات

طرق اختراق الشبكات	Count	Pct of Responses	Pct of cases
نظم داخلية (من داخل البنك)	65	27.4	36.9
من خلال فروع البنك المختلفة	47	19.8	26.7
من خلال الانترنت	125	52.7	71.0
Total responses	237	100.0	134.7

3 Missing cases:176 valid cases

اولاً الأنترنت :- من أهم الأشياء التي يتميز بها عصرنا هى كثرة المعلومات فقد أشارت الدراسات الإستراتيجية إلى أن مقدار المعلومات المنتجة في السنوات العَشرة الأخيرة فقط تعادل ما أنتجته البشرية من معلومات طوال الحقب الزمنية المنصرمة (١٩)، بمعنى أن كل عشر سنوات في عصر المعلومات وربما أقل في المستقبل تكفي لمضاعفة حجم المعلومات التي تنتجها البشرية و يرجع ذلك فى المقام الاول لتوسع شبكة الإنترنت.

فقد تجاوز عدد مستخدمي الإنترنت في العالم عدد المليار مستخدم لأول مرة في ديسمبر من العام وتتصدرا الصين اكبر عدد من مستخدمي الإنترنت إذ بلغ عدد المستخدم ٢٩٨مليون مستخدم , تليها في المرتبة الثانية الولايات المتحدة ب ١٦٣ مليون مستخدم وجاءت اليابان في المرتبة الثالثة بعدد ٦٠ مليون مستخدم. (٢٠) هذا الكم الهائل من المستخدمين أدى الى عدد من المخاطر عند الاتصال بشبكة الإنترنت فعند استخدام بطاقات الائتمان الخاصه عبر الإنترنت يمكن ان يحصل طرف اخرعلى ارقام هذه البطاقه .كما يمكن ان تكون مواقع البيع عبر الانترنت مواقع زائفة .

على حسب عينة الدراسة فقد جاءت طرق الإختراق عبر الإنترنت بتكرار١٢٥ ونسبة بلغت ٧١,٠٪ و تمثل هذه النسبه اكبر نسبة من طرق اختراق الشبكات .

ثانياً النظم الداخلية :- معظم الأنظمة الأمنية تقوم على حماية الشبكات من الإختراقات الخارجية ولكن هناك جانب مهم يتمثل في الموظفين المحليين الذين يمتلكون معلومات دقيقة عن تلك الأنظمة وكيفية عملها.

فعند تصميم نظام أمنى يجب الوضع في الإعتبار هؤلاء الموظفين المحليين ومراقبتهم كما يمكن تطبيق إجراءات وقائية تمنع اى موظف التواجد في غير المكان المخصص له كما يجب أن يلتزم كل موظف الطابق الذي يعمل به وبتطبيق هذا النظام نحد من الإختراقات المحلية التي تحدث من داخل المؤسسة . وعلى حسب أفراد عينة الدراسة فأن الطرق التي يمكن أن يتم من خلالها اختراق الشبكة جاءت النظم الداخلية فى المرتبة الثانية بنسبة ٣٦,٩٪ وتكرار بلغ٦٥.

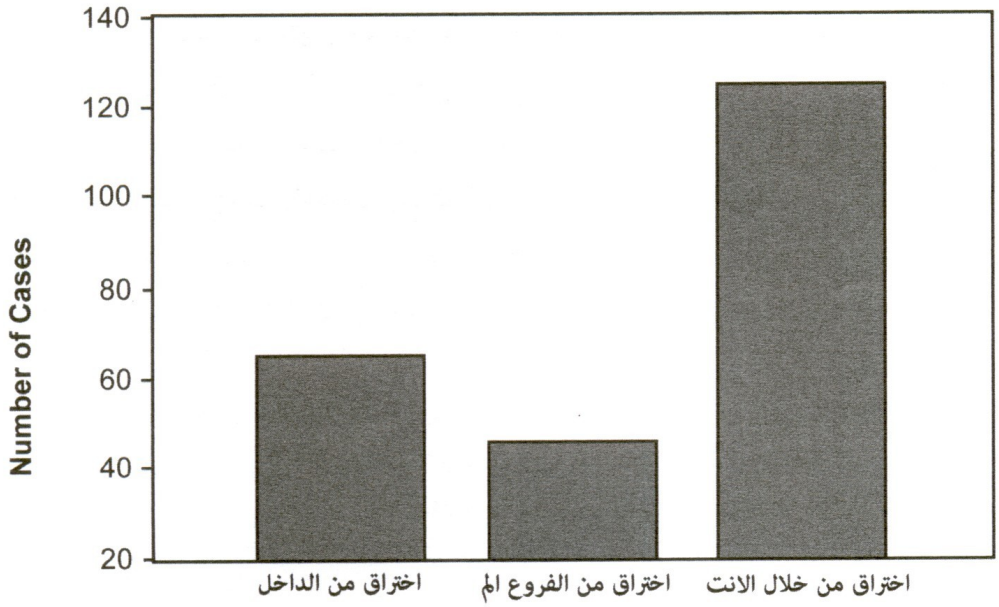
ثالثاً الفروع :- معظم المصارف السودانية لديها فروع مختلفة في معظم الولايات كما يوجد لدى بعض البنوك فروع خارج القطر وذلك لتسهيل ربط العميل أثناء سفره بالخارج وتأتى هذه الفروع بجوانب ايجابية كثيرة لا تخفى على اى احد فيمكن الاستفادة منها فى تقديم الخدمة في اى مكان يحتاج لها العميل.

ولكن تلك الفروع تتسبب في بعض المشاكل ,فكلما كبرحجم المؤسسة صعب التحكم والسيطرة عليها وزادت المشاكل والاختراقات في تلك الشبكة التي تربط هذه الفروع مع بعضها ومن هنا يأتى السؤال في كيفية التحكم في تلك الفروع وكيفية تأمين المعاملات المرسلة والمستقبلة من خلالها.

ولتأمين عملية الاتصال بين الفروع يمكن يمكن تطبيق عدد من الاجراءات من خلال عمل شبكة خاصة افتراضية (VPN) بين تلك الفروع المختلفة وذلك لتأمين خطوط الاتصالات بين كل الفروع وتأتي أهمية هذه الشبكة في إنها تقوم بتأمين كل المعلومات المتبادلة بين أطراف الشبكة حيث يتم نقلها من خلال قناة تشفير سواء كانت هذه المعلومات تنتقل من خلال خدمة نقل الملفات FTP أو البريد الالكتروني SMTP وصفحة الويب أو غيرها من خدمات النقل الأخرى. كما توجد تقنيات تأمين اخرى كأنظمة الجدران النارية وتشفير البيانات المرسلة

وعلى حسب عينة الدراسة تم اختيار فروع البنك المختلفة بتكرار بلغ ٤٧ وبنسبة ٣٦,٩٪ و يأتى هذا الخيار فى المرتبة الثالثة من طرق الهجوم على الشبكة

شكل(٤) يوضح طرق اختراق الشبكات



٩- الخلاصة

من خلال ماتم التطرق له من تحليل لعدد من مخاطر المصارف المالية وعلى حسب آراء العينة المدروسة جاءت الأصول المادية كأهم الأصول التى تحتاج للحماية فى شبكة البنوك, اما الغرض من الهجوم على الشبكات كان دمار البرامج كأعلى فرض من فرضيات الدراسة ,وكان المنافسون هم من اكثر نوعية مهاجمين الشبكات على البنوك ,أما الإختراق من خلال الانترنت كان من اكثر الطرق التى يمكن ان يتم من خلالها الهجوم على شبكات المصارف المالية.

ونظراً لما يصاحب إجراء العمليات المصرفية الإلكترونية وإصدار وسائل دفع لنقود الكترونية من مخاطر متعددة لاتقتصر فقط على المخاطر التقليدية، يستلزم الأمر وضع الأسس للإدارة الحصيفة لهذه المخاطر والتحديد الدقيق لمسؤوليات مختلف الجهات ذات العلاقة بها وما يستلزمه ذلك من قيام اتحاد المصارف العربية ومؤسساته بإستنباط معايير عالمية تختص بالبنوك والمصارف المالية وذلك فيما يتصل بالمال الإلكتروني وتقنيات الخدمات المصرفية والمالية وفي مقدمتها البطاقات المالية ونظم التحويل الإلكتروني والعمل المصرفي والمالي , مع الأخذ فى الأعتبار الإطار القانوني للعمل المصرفي في بيئة الإنترنت ،مع العلم بأنه لايوجد أى قانون يتعلق بالبنوك الالكترونية والأئتمانات المصرفية عدا عدد من النصوص التي تضمنتها قوانين التجارة الالكترونية .

وتحديد الإحتياجات الفعلية للمصارف في مجال أمن المعلومات, عن طريق تصميم برامج تخصصية عالية المستوى تتوافق مع تلك الإحتياجات, وتسهم فيها جميع مؤسسات المجتمع التعليمية والمنظمات الإقليمية والقطاع الخاص.

ودعوة المؤسسات المالية والمصرفيه إلى تطوير وتوحيد المعايير الأمنية ومستلزماتها الرقابية والتدقيقية بهدف الوصول إلى تحقيق المحول الوطني للربط بين المصارف المختلفة. والعمل على وضع معايير وضوابط لحماية خصوصية وسرية البيانات المتبادلة بين المصارف المختلفة الداخلية والتبادلات الخارجية منها.

المراجع

(١) نعيم دهمش، ظاهر شاهر القشي، مخاطر العمليات المصرفية التي تتم من خلال القنوات الالكترونية،مجلة البنوك العدد الثاني، المجلد الثالث والعشرون، اذار ٢٠٠٤، الاردن.

(٢) جمال محمد غيطاس , امن المعلومات والامن القومى، نهضة مصر للطباعة و النشر والتوزيع، ٢٠٠٧

(٣) هيثم المسيري- خدمات مواقع البنوك الاكترونية، ورقة عمل مقدمة فى ندوه الخدمات البنكيه الالكترونيه الشامله (روية مستقبليه) ـ مصر ٢٠٠٧

(٤) يونس عرب، التشريعات والقوانين المتعلقة بالانترنت بالدول العربية، (ورقه عمل مقدمه في مؤتمر ومعرض التكنولوجيا المصرفية العربية والدولية اتحاد المصارف العربية) الأردن ٢٠٠٣ - المصدر http://www.arablaw.org/Download/Internet_Legislation_Article.doc

(٥) خالد بن سليمان الغثبر,الواقع الامني والتقني للخدمات البنكية ,جريده الاقتصاد الالكترونية - المصدر http:\\ coeia.edu.sa//index.php/ar/about-coeia/management-strucure.html تاريخ الاطلاع ٢٠٠٩

(٦) توم توماس، الخطوة الاولى نحو امان الشبكات، الدار العربية للعلوم، ٢٠٠٤

(٧) تقرير المانى منقول من وكالة الانباء رويترز٢٠٠٦ –المصدر Arabic.cnn.com/scitech.html تاريخ الاطلاع ٢٠٠٩

(٨) محمد دباس الحميد، ماركو ابراهيم نينو، حماية انظمة المعلومات، دار الحامد للنشر والتوزيع، ٢٠٠٧

(٩) محمد عبد اللة القاسم، عبد الرحمن عبد العزيز الحمدان، اساسيات امن المعلومات، مكتبة الملك فهد الوطنية اثناء النشر، ٢٠٠٨

(١٠) يعقوب السليمان، أمن المعلومات البنكية الإلكترونية، (ورقة عمل مقدمة لمؤسسة النقد العربي السعودي)، المملكة العربية السعودية ٢٠٠٥ - المصدر http://www.itsecurityforum.org.sa/presantations/SAMA.zip ، تاريخ الاطلاع ٢٠٠٩

(١١) عزة على محمد الحسن، الجوانب القانونية للصريفة الاكترونية، ٢٠٠٩، بدون ناشر

(١٢) أسعد أبو خليل، جريمة خارقة، مجلة العرب الاسوبوعى، السبت ١٥-٨ -٢٠٠٩

(١٣) جريده الشرق الاوسط، العدد (٨١٦٨)، ٢٠٠١, - المصدر: http://www.aawsat.com/default.asp تاريخ الاطلاع ٢٠٠٨

(١٤) مجلة الاهرام للكمبيوتر والانترنت والاتصالات، لغة العصر، العدد الثالث والسبعون، ٢٠٠٧

(١٥) عزة على محمد الحسن،الجريمة المعلوماتية فى القانون السودانى، ٢٠٠٩، بدون ناشر

(١٦) وكالة سونا للانباء، المصدر جريدة الدار العدد (٤٧١٥)، ٢٠٠٨