بسم الله الرحمن الرحيم

المعهد العالي للدراسات المصرفية والمالية

أمانة البحوث والتوثيق

المنتدى المصرفي الخمسون

الصيرفة الإلكترونية الآمنة
Secure eBanking

إعداد

د. نور الدين عبد الرحمن نور الدين

كلية علوم التقانة

أبريل 2003م

الصيرفة الإلكترونية الآمنة
Secure eBanking

مستخلص الورقة:

يلاحظ أن بنية المعلومات التي يمثلها الإنترنت في تصاعد مستمر، حيث وفرت هذه البنية الارتباط العالمي وسهلت من عملية الاتصال وبثمن زهيد. وعلى اثر ذلك، اصبح الإنترنت يمثل سوقاً رائجة وجاذبة لعارضي السلع ومقدمي الخدمات ومن بينها التجارة الإلكترونية عبر الوب (WEB) والتي تعتبر واحدة من أهم الخدمات التي يوفرها الإنترنت لمستخدميه.

تنبع جاذبية السوق الإلكترونية من خلال تمكينها للمصارف من الوصول لعملائها – عبر الإنترنت – في كافة أنحاء المعمورة، ويستطيع العملاء بدورهم إنجاز معاملاتهم المصرفية من إيداع وسحب وغيرها من أي مكان إليكترونياً. ومن هنا جاء مصطلح الصيرفة الإلكترونية (البنك الإلكتروني). وباعتبار أن الإنترنت يمثل وعاء للمعلومات وأداة اتصال عالمية، يتعين علي المصارف النظر بجدية في كيفية الإفادة من هذه الإمكانيات، وذلك:

– أما باستخدام الإنترنت لتقديم الخدمات المصرفية عالمياً.

– وأما باستخدام الإنترنت للأغراض الداخلية للمصرف.

إن العلاقة ما بين المصارف والإنترنت يمكن لها أن تأخذ أشكالاً مختلفة، فمن الممكن أن يرتبط المصرف بالإنترنت فقط من أجل أن يجعل مستخدميه يفيدون من خدمات الإنترنت كالبريد الإلكتروني ونقل الملفات وتصفح المواقع. كما يمكن للمصرف أن ينشئ موقع دعائي علي شبكة الوب يعرض فيه المعلومات العامة عن المصرف والخدمات التي يقدمها، بحيث يمكن أن يعمل هذا الموقع من علي مخدم داخل المصرف أو خارجه.

هذا، وتكون العلاقة أكثر عضوية ما بين المصرف والإنترنت عندما يقدم المصرف خدماته لعملائه عبر الإنترنت بشكل مباشر أو أن يصبح جزءً من منظومة مصرفية تقدم خدماتها لزبائنها عبر الإنترنت. وأياً كان شكل الارتباط بين المصرف والإنترنت، فإن قضية الأمن هي الشاغل الأساسي نتيجة للطبيعة المفتوحة للإنترنت والمخاطر المتعددة التي تنشأ عن استخدامه. ولذلك، فإن المصارف مواجهة بالنظر في هذه القضية وإيجاد الحلول المناسبة لها وفقاً لشكل الارتباط بالإنترنت.

تتمثل المخاطر الرئيسية لاستخدام الإنترنت في إمكانية فقدان عناصر الأمن الأساسية التالية:

1) الخصوصية (السرية): والمعني بها أن تظل المعلومات والبيانات المتعلقة بالعملاء ومعاملاتهم خاصة بهم فقط.

2) التكاملية: والمعني بها أن يتم حفظ البيانات والمعلومات المتعلقة بالمصرف وعملائه بحيث لا يمكن تغييرها أو تبديلها إلا من قبل المخول لهم ذلك.

3) التوفر: والمعني بها أن يظل المصرف قادراً علي تقديم الخدمات الإلكترونية لعملائه في كل الوقت.

إن توفير متطلبات الأمن المشار إليها أعلاه، لا يتحقق إلا بتبني المصرف لبرنامج لتأمين المعلومات والارتباط بالإنترنت، بحيث يحدد هذا البرنامج بوضوح المسؤوليات والإجراءات التي يجب اتخاذها من أجل تحقيق أهدافه. وهذا الأمر يستلزم يتطلب إتباع مجموعة من الخطوات تتمثل في:

– إنشاء سياسة أمنية تحدد الرؤية الشاملة للمصرف حيال قضية الأمن.

– تحديد وتسمية الجهات المسئولة عن تنفيذ ومتابعة وتأهيل برنامج تأمين المعلومات.

– تحديد المخاطر وكيفية إدارتها.

– تطبيق تقنيات الأمن اللازمة لتحقيق مستوي الأمن المطلوب.

– مراقبة أداء تقنيات الأمن والتحقق من استتباب الأمن.

– تدريب وتأهيل العاملين في المصرف في مجال أمن المعلومات.

1.0 Introduction

The Internet is a rapidly evolving information infrastructure, which provides global connectivity, easy reachability and interactive communications at moderate cost for the consumer. The dominating application is the World Wide Web (WWW), with its potential of millions of connected computer systems. Currently, WWW is primarily used to provide easy access to free-of-charge information (typically research or marketing information). But this is expected to change dramatically in the near future. WWW is now starts to provide a basis for electronic commerce and trade

Hence, the Internet has reached an increased market potential which makes it attractive for all service providers and, in particular, for the banks. With the Internet, banks can easily reach their customers on a global scale. Customers may sign up electronically, may order electronically, and may transfer money electronically from almost any place in the world; such bank electronic activities are conventionally called ebanking. However, as the Internet is a highly open and distributed infrastructure without central regulation and control, it is mandatory that the banks carefully address and solve the security issues related to banking applications over the Internet.

Banks must position themselves regarding:

- the use of the Internet for global banking services,
- the use of the Internet for internal purposes,

2.0 Banks and the Internet (Relevant Scenarios)

A bank may find itself in a number of different roles with different security requirements when it comes to using the Internet or, to providing financial services on the Internet. This section will describe the relevant scenarios. [1]

2.1 The bank as a user of the Internet (Scenario 1)

The bank may be a user of the Internet, that is, it may be interested in connecting to the Internet in order to allow its employees to exchange e-mail, to use file transfer, or to browse Web sites. In such a scenario, the bank is concerned that its internal systems become vulnerable to attacks from the Internet by hackers, viruses, and the like. A firewall is typically used to isolate the internal systems from the Internet.

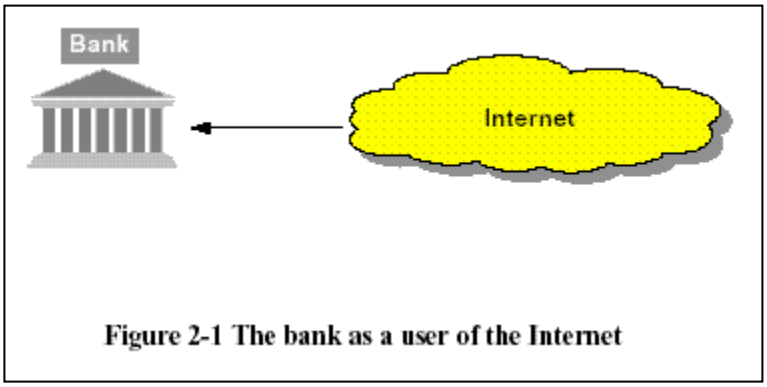

Figure 2-1 The bank as a user of the Internet

2.2 The bank as an information provider (Scenario 2)

The bank may be an information service provider on the Internet, that is, the bank may be interested in connecting to the Internet in order to provide public information about its services (e.g. use the Internet for marketing purposes). Typically, static information is displayed and the bank does not want to restrict access to the information. From a security point of view, this scenario is uncritical and is widely used. The bank may either install an isolated Internet Web server (Insource) or may even buy a few pages on an Internet Web server of an external service provider (Outsource).

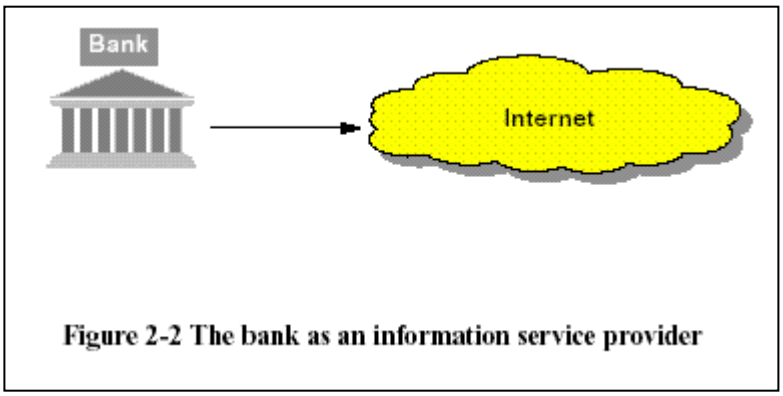

Figure 2-2 The bank as an information service provider

2.3 The bank as an electronic banking provider (Scenario 3)

The bank may be an electronic banking service provider on the Internet. The electronic banking services are typically separated into **home banking** and **corporate banking**. The Internet is seen as a way to cost-effectively reach the customer. In a home banking scenario, security requirements are paramount. **User authentication**, **confidentiality**, and **digital signatures** on payment orders are customary requirements.

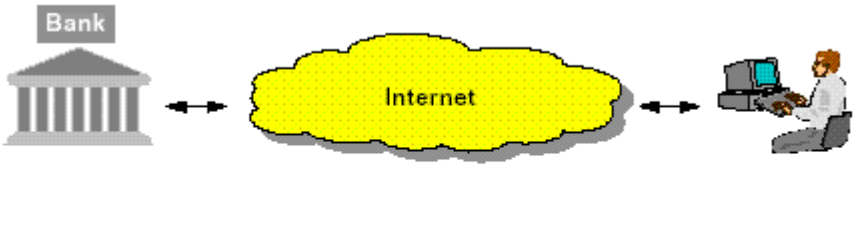

Figure 2-3 The bank as an electronic (home) banking provider

2.2.4 The bank as a part of an electronic payment system (Scenario 4)

The bank may be part of an electronic payment system to be used on the Internet. Such payment systems are needed to allow for electronic commerce. Various electronic payment systems, such as credit card schemes, electronic cash schemes, and purse schemes, will co-habitate on the Internet.

Banks will play different roles in the various payment schemes. Security requirements vary from scheme to scheme, but are typically high and demand the usage of sophisticated **cryptographic algorithms.**

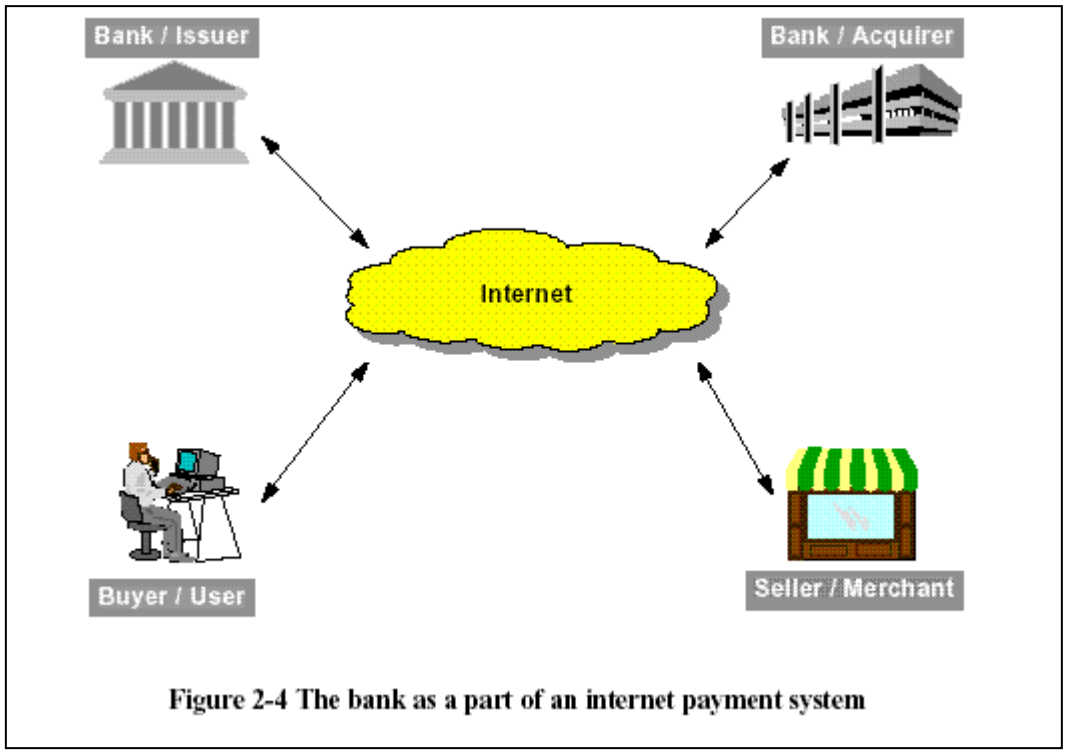

Figure 2-4 The bank as a part of an internet payment system

3.0 Threats

3.1 Introduction

It is the responsibility of banks to undertake a risk analysis to determine the threats to their business integrity and the security of their customers. However, a risk analysis, even if rigorous and thorough, will not provide a complete picture.

The threats outlined below are those that arise when conducting business remotely across an insecure electronic network such as the Internet [1].

(a) Threats leading to an impact on the service provider (The Bank)

- Funds transfers initiated by an imposter
- Loss of reputation through fake server.
- Customer falsely denies having issued payments instruction(s).
- Disclosure of confidential customer data to an outside party.
- Loss of data on 'valuable customers' to a competitor.
- Loss of security in the central system (intruder, virus, DOS).

(b) Threats leading to an impact on the customer

- Funds transfer initiated by an imposter.
- Loss of privacy of customer financial data. Loss of confidentiality of other private data.
- Unauthorized access to credit information by a third party.
- Financial institution falsely denies having received (or not having received) instructions.

(c) Additional risk factors

- Security features often reduce 'ease of use'. Customers cannot cope with many different PINs, passwords or other security procedures.
- Export and usage restrictions on strong cryptography.
- Reluctance to download information or software which has not been authenticated by a trusted party.

4.0 Security Requirements

4.1 Information Security Program

To provide secure ebanking, all risks outlined above should be eliminated. Providing confidentiality (privacy), integrity, availability and non-repudiation can only achieve this secure environment. Thus bank management shall, through an effective **Information Security Program**:

- assure the security and confidentiality of customer records and information as well as the proprietary records and information of the bank;
- protect against any anticipated threats or hazards to the security or integrity of such records and information; and
- protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer or the bank [2].

The Program shall use appropriate administrative, technical, and physical safeguards to protect customer records and information as well as the bank's own proprietary information

4.1.1 Information Security program Objective

The objective of information security program is "the *protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity*" [3].

For any bank, the security objective is met when:

- information systems are available and usable when required (availability);
- data and information are disclosed only to those who have a right to know it (confidentiality); and
- data and information are protected against unauthorized modification (integrity). The relative priority and significance of availability, confidentiality, and integrity vary according to the data within the information system and the business context in which it is used.

4.1.2 Core Principles

The security program objective is supported by the following eight core principles[3].

Accountability: Responsibility and accountability must be explicit. Security of information requires an express and timely apportionment of responsibility and accountability among data owners, process owners, technology providers, and users. This accountability should be formalized and communicated.

Awareness: Awareness of risks and security initiatives must be disseminated. In order to foster confidence in information, data owners, process owners, technology providers, users, and other parties, with a legitimate interest to learn or be informed, must be able to

gain knowledge of the existence and general extent of the risks facing the organization and its systems and the organization's security initiatives and requirements. Security measures are only effective if all involved are aware of their proper functioning and of the risks they address.

Multidisciplinary: Security must be addressed taking into consideration both technological and non-technological issues. Security is more than just technology. It also covers administrative, organizational, operational, and legal issues. Accordingly, technical standards should be developed with and, be reinforced by, codes of practice; audit; legislative, legal, and regulatory requirements; and awareness, education, and training.

Cost Effectiveness: Different levels and types of security may be required to address the risks to information. Security levels and associated costs must be compatible with the value of the information

Integration: Security must be coordinated and integrated. Measures, practices, and procedures for the security of information should be coordinated and integrated with each other and with other measures, practices, and procedures of the organization, and third parties on whom the organization's business processes depend, so as to create a coherent system of security.

Reassessment: Security must be reassessed periodically. The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time

Timeliness: Security procedures must provide for monitoring and timely response. Banks must establish procedures to monitor and respond to real or attempted breaches in security in a timely manner in proportion with the risk.

Societal Factors: Ethics must be promoted by respecting the rights and interests of others. Information and the security of information should be provided and used in such a manner that the rights and interests of others are respected and that the level of security must be consistent with the use and flow of information that is the hallmark of a democratic society

4.2 Approach to achieve Security

To meet the security objective and develop and maintain adequate controls in compliance with generally accepted core principles, the following integrated approach is necessary.

Policy Development:

The security objective and core principles provide a framework for the first critical step for any organization – developing a security policy. Security Policy represents the overall bank's view to security.

Roles and Responsibility

The bank's Chief Information Officer (CIO) is assigned primary responsibility for the development, implementation, and maintenance of the Program. To assist, the CIO may convene a committee of other bank managers from various divisions or departments of the bank. At least annually, the CIO will report to the Board of Directors the overall status of the Program. The report shall discuss material matters related to the Program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the Program.

Identifying Risks

Management shall identify the reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Further, management shall develop and implement procedures and other controls that take into account the likelihood and potential damage of these threats.

Managing Risks

Management shall develop, implement, and maintain the Program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities.

Management has, as of today, identified the following security measures appropriate for the bank and either has or will shortly adopt those measures that management concludes are appropriate. Testing methods are also listed [2].

Control	Purpose/ Description	Bank Policy or Procedure Cross-Reference	Testing
Access controls on customer information systems	Includes controls to: Authenticate and permit access only to authorized individuals and Controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means	The following Bank policies and procedures address controls on access: - PC/LAN Security Policy - Internet/Email Policy - Firewall Policy - Network Security Administrator's Procedures - Ethics and Employee Conduct for Personal Use of Information Resources	Outside Audit Firm annual review of Internal Security and Controls. Annual penetration testing by third party, (name them
Encryption of electronic customer information	Includes information while in transit or in storage on networks or systems to which unauthorized individuals may have access.	The following provide methods of encryption of electronic customer information: -VPN Technology for secure communication - SSL technology for on-line banking - PGP and password procedures for email and internal communications	During the annual Outside Audit Firm Controls Review audit, the SSL connections will be tested along with a review of emails for PGP usage
Monitoring systems and procedures	to detect actual and attempted attacks on or intrusions into customer/bank information systems	- NIDS technology to detect intrusion - Monthly Log Reviews by Network Security Administrator	Audit of I.S. Controls will review the log sheet of the Network Security Administrator
Incident Response program	that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems.	Specified in security policy procedures	The Network Security Administrator will update the response procedures
Contingency and Disaster Recovery	Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures	- Disaster Recovery Plan - Business Continuity Plan (Systems) with mirrored system capability.	Testing of the disaster recovery plan and the business continuity plan will be performed and documented by I.S. Department on an annual basis

Monitoring: Monitoring measures need to be established to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified,

investigated, and acted upon, and to ensure ongoing compliance with policy, standards, and minimum acceptable security practices.

Awareness, Training, and Education: Awareness of the need to protect information, training in the skills needed to operate information systems securely, and education in security measures and practices are of critical importance for the success of an organization's security program.

5.0 Conclusion

With the ever changing technological environment, what is considered state-of-the-art today will be obsolete tomorrow, and security must keep pace with these changes. Security must be considered as an integral part of the ebanking. Security must be dealt with in a proactive manner in order for it to be effective.

References

[1] "Secure banking over the Internet", TR 401, European Committee for Banking Standards. March 1997, Avenue de Tervueren, 12, 1040, Brussels. http://www.ecbs.org/publications/security.htm#DocsTC4

[2] "Information Security Policy", www.bankersonline.com

[3] "Managing Information Security", The Institute of Internal Auditors, http://www.theiia.org/ecm/tech.cfm?doc_id=849

1.0 مقدمة

إنّ الإنترنت a بناء معلومات تحتي ناشئ بسرعة، الـذي يـزوّد ربـط عـالمي، reachability سـهل وإتصالات تفاعلية في الكلفة المعتدلة للمستهلك. سيطرة على التطبيق الشبكة العالمية (دبليو دبليو دبليـو)، بإمكانيته من ملايين أنظمة الحاسوب المرتبطة. حاليا، شبكة عالمية أوليا تستعمل لتزويد الوصول السـهل لتحرير من معلومات التهمة (يبحث نموذجيا أو يسوّق معلوماتا). لكن هذا يتوقّع تغيير بشـكل مثيـر فـي المستقبل القريب. الشبكة العالمية تبدأ توفير الآن a قاعدة للتجارة عبر الإنترنت وtrad

لذلك، وصلت الإنترنت إمكانية سوق متزايدة التي تعملهو جذّابة لكلّ مجهزون الخدمة، وبشـكل خـاص، للبنوك. بالإنترنت، بنوك يمكن أن تصل زبائنهم بسهولة على a مقيـاس عـالمي. الزبـائن قـد يوقّعـون إلكترونيا، قد يطلب إلكترونيا، وقد يحوّل مال إلكترونيا من تقريبا أيّ مكان في العالم؛ مثل هـذا نشـاطات مصرف الإلكترونية تدعو ebanking بشكل تقليدي. على أية حال، كالإنترنت a مفتوحة جـدا ووزّعـت بناء تحتي بدون تعليمة وسيطرة مركزية، هو إلزامية التي تخاطب البنوك بعناية وتحـلّ القضـايا الأمنيـة تعلّقت بالتطبيقات المصرفية على الإنترنت.

البنوك يجب أن تضع أنفسهم بخصوص:

- إستعمال الإنترنت للخدمات المصرفية العالمية،
- إستعمال الإنترنت للأغراض الداخلية،

2.0 بنك والإنترنت (سيناريوهات ذات العلاقة)

أي مصرف قد يجد نفسه في عدد من الأدوار المختلفة بمتطلبات الأمن المختلفـة عنـدما يتعلـق الأمـر بتستعمل الإنترنت، أو إلى تزويد الخدمات المالية على الإنترنت. هذا القسم سيصـف السـيناريوهات ذات العلاقة. [1]

2.1 المصرف كمستعمل الإنترنت (سيناريو 1)

المصرف قد يكون مستعمل الإنترنت، تلك، هو قد يهتمّ بالإتصال بالإنترنت لكي يسمح لمستخدميه لتبـادل البريد الإلكتروني، لإستعمال ارسال الملفات، أو لتصفّح مواقع الويب. في مثل هذا السـيناريو، المصـرف قلق بأن أنظمته الداخلية تصبح عرضة للهجمات من الإنترنت من قبل لصوص الكومبيـوتر، فيروسـات، وما شابه. أي برنامج حماية نموذجيا يستعمل لعزل الأنظمة الداخلية من الإنترنت.

2.2 المصرف كمجهز معلومات (سيناريو 2)

المصرف قد يكون مجهز خدمات معلوماتية على الإنترنت، تلك، المصرف قد يهتمّ بالإتصال بالإنترنت لكي يزوّد معلومات عامة حول خدماته (ومثال على ذلك: – يستعمل الإنترنت للأغراض التسويقية). نموذجيا، معلومات ساكنة تعرض والمصرف لا يريد تحديد الوصول إلى المعلومات. من a وجهة نظر أمن، هذا السيناريو غير ناقد وكثير الإستعمال. المصرف قد أمّا يركّب خادم ويب الإنترنت معزول (إنسورس) أو قد يشتري بضعة صفحات حتى على خادم ويب الإنترنت مجهز خدمة خارجي (وتسورس).

2.3 المصرف كمجهز مصرفي إلكتروني (سيناريو 3)

المصرف قد يكون مجهز خدمة مصرفي إلكتروني على الإنترنت. إنّ الخدمات المصرفية الإلكترونية تفصل نموذجيا إلى الصيرفة البيتية والأعمال المصرفية المتعلّقة بالشركات. إنّ الإنترنت ترى كaطريق لوصول الزبون بشكل مربح. في a سيناريو صيرفة بيتية، متطلبات أمن أساسية. تحقّق مستعمل، سريّة، وتواقيع رقمية على أوامر الدفع متطلبات مألوفة.

2.2.4 المصرف كaجزء نظام دفع إلكتروني (سيناريو 4)

المصرف قد يكون جزء نظام دفع إلكتروني الّذي سيستعمل على الإنترنت. مثل هذه أنظمة الدفع تحتاج للسماح للتجارة عبر الإنترنت. أنظمة الدفع الإلكترونية المختلفة، مثل مخططات بطاقة الإئتمان، مخططات نقد إلكترونية، ومخططات محفظة، سشركاء habitate على الإنترنت.

البنوك ستلعب أدوار مختلفة في مخططات الدفعة المختلفة. تتفاوت متطلبات الأمن من المخطط إلى المخطط، لكن عالي نموذجيا وتطلب إستعمال الخوارزميات المشفّرة المتطوّرة.

3.0 تهديد

3.1 مقدمة

هي مسؤولية البنوك لتعهّد a تحليل أخطار لتقرير التهديدات إلى سلامة عملهم وأمن زبائنهم. على أية حال , a تحليل أخطار، حتى إذا صارم وشامل، سوف لن يزوّد a يكمل صورة.

التهديدات تجدون بالتفصيل أدناه أولئك الذي يظهر متى يجري عملا عن بعد عبر شبكة إلكترونية غير آمنة مثل الإنترنت [1].

(a) تهديدات التي تؤدّي إلى تأثير على مجهز الخدمة (المصرف)

- يموّل الإنتقالات بدأت بـimposter
- خسارة السمعة خلال الخادم المزيف.
- ينكر زبون بشكل خاطئ بعد أن أصدر أمر الدفعات (s).
- كشف بيانات الزبون السرّية إلى خارج الحزب.
- خسارة البيانات على ' زبائن ثمين إلى a منافس.
- خسارة الأمن في النظام المركزي (دخيل، فيروس، دوس).

(b) تهديدات التي تؤدّي إلى تأثير على الزبون

- يموّل نقلا بدأ بـimposter.
- خسارة سرية بيانات الزبون المالية. خسارة سريّة أخرى البيانات الخاصّة.
- وصول غير مخوّل لتصديق المعلومات من قبل a طرف ثالث.
- تنكر مؤسسة مالية بشكل خاطئ بعد أن إستلمت (أو لم تستلم) الأوامر.

(c) عوامل خطر إضافية

- تخفّض ميزّات الأمن في أغلب الأحيان ' سهولة الإستعمال '. الزبائن لا يستطيعون تحمّل الكثير الدبابيس المختلفة، كلمات سر أو إجراءات أمن أخرى.
- قيود الإستعمال والتصدير على الكتابة المشفّرة القوية.
- تردّد لتحميل المعلومات أو البرامج التي ما كانتا حقّق من قبل a حزب مؤتمن.

4.0 متطلب أمن

4.1 برنامج أمن معلومات

لتزويد ebanking آمن، كلّ الأخطار لخّصت فوق يجب أن تزال. تزويد السريّة (سرية)، سلامة، توفر وغير نبذ يمكن فقط أن ينجز هذه البيئة الآمنة. هكذا يودع الإدارة س، خلال برنامج أمن معلومات فعّال:

· يطمأن الأمن وسريّة السجلات ومعلومات الزبون بالإضافة إلى السجلات الإمتلاكية ومعلومات المصرف؛

· يحمي ضدّ أيّ تهديدات أو أخطار متوقّعة إلى الأمن أو سلامة مثل هذه السجلات والمعلومات؛ و

· يحمي ضدّ الوصول الغير مخوّل إلى أو إستعمال مثل هذه السجلات أو المعلومات التي يمكن أن تؤدّيا إلى أذى كبير أو تزعجان إلى أيّ زبون أو المصرف [2].

البرنامج سيستعمل وقاية طبيعية وتقنية وإدارية ملائمة لحماية السجلات ومعلومات الزبون بالإضافة إلى معلومات المصرف الخاصة الإمتلاكية

4.1.1 هدف برنامج أمن معلومات

إنّ هدف برنامج أمن المعلومات "حماية مصالح تلك إعتماد على المعلومات، وأنظمة وإتصالات المعلومات التي تسلّمان المعلومات، من الأذى ينتج من حالات فشل التوفر، سريّة، وسلامة "[3].

لأيّ مصرف، هدف الأمن يقابل متى:

· أنظمة معلومات متوفرة وصالح للإستعمال عندما مطلوب (توفر)؛

· بيانات ومعلومات معلنة فقط إلى أولئك الذين لهم a حقّ لمعرفته (سريّة)؛ و

· بيانات ومعلومات محمية ضدّ التعديل الغير مخوّل (سلامة). إنّ الأولوية النسبية وأهمية التوفر، سريّة، وتتفاوت سلامة طبقا للبيانات ضمن نظام المعلومات وسياق العمل في أي هو مستعمل.

4.1.2 مبدأ رئيسي

إنّ هدف برنامج الأمن مدعوم من قبل المبادئ الرئيسية التالية الثمانية 3].

المسؤولية: المسؤولية والمسؤولية يجب أن تكونا واضحة. يتطلّب أمن المعلومات تقسيم سريعا ومناسب من المسؤولية والمسؤولية بين مالكي البيانات، مالكو عملية، مجهزون تقنية، ومستعملون. هذه المسؤولية يجب أن تشكّل وتتّصل.

الوعي: وعي مبادرات الأمن والأخطار يجب أن ينشرا. لكي يتبنّى ثقة في المعلومات، مالكو بيانات، مالكو عملية، مجهزون تقنية، مستعملون، وأطراف أخرى، مع a يشرّع الإهتمام لتعلّم أو ليكن في علمكم، يجب أن يكون قادر على كسب معرفة الوجود والمدى العامّ من الأخطار التي تواجه المنظمة وأنظمتها ومبادرات ومتطلبات أمن المنظمة. التدابير الأمنية فعّالة فقط إذا كلّ المعقّد مدركة لإشتغالهم الصحيح والأخطار يخاطبون.

متعدّد تأديبي: الأمن يجب أن يخاطب أخذ بنظر الإعتبار كلتا قضايا تقنية وغير تقنية. الأمن أكثر من فقط تقنية. يغطّي شغّال تنظيمي إداري أيضا، ومسائل قانونية. وفقا لذلك، معايير تقنية يجب أن تطوّر مع، وتكون مدعومة من قبل، قواعد ممارسة؛ التدقيق؛ المتطلبات التنظيمية والقانونية والتشريعية؛ ووعي، تعليم، وتدريب.

تأثير كلفة: المستويات المختلفة وأنواع الأمن قد يتطلّبان لعنونة الأخطار إلى المعلومات. الأمن يستوي وكلف مرتبطة يجب أن تكون متوافقة بقيمة المعلومات

التكامل: الأمن يجب أن ينسّق ويكامل. الإجراءات، ممارسات، وإجراءات لأمن المعلومات يجب أن تنسّق وتكامل مع بعضهم البعض وبالإجراءات الأخرى، ممارسات، وإجراءات المنظمة، وأطراف ثالثة على من عمليات عمل المنظمة تعتمد، لكي يخلق a نظام متماسك من الأمن.

إعادة تقييم: الأمن يجب أن يقيّم ثانية بشكل دوري. أمن أنظمة المعلومات يجب أن يقيّم ثانية بشكل دوري، كأنظمة معلومات والمتطلبات لأمنهم يتفاوتان بمرور الوقت

تيميلنيس: إجراءات أمن يجب أن تزوّد لمراقبة والردّ المناسب. البنوك يجب أن تؤسّس الإجراءات لمراقبة وردّ على الخروقات الحقيقية أو المحاولة في الأمن بطريقة مناسبة في النسبة بالخطر.

العوامل الإجتماعية الحضارية: الأخلاق يجب أن تروّج لها بإحترام الحقوق ومصالح الآخرين. المعلومات وأمن المعلومات يجب أن يزوّدا ويستعملا في مثل هذا الإسلوب الذي الحقوق ومصالح الآخرين تحترمان والتي مستوى الأمن يجب أن يكون متّسق مع الإستعمال وتدفق المعلومات الذي علامة a مجتمع ديمقراطي

4.2 نظرة لإنجاز الأمن

لمقابلة الأمن موضوعية ويطوّر ويبقي سيطرة كافية في الإلتزام بالمبـــادئ الرئيســـية المقبولـــة عمومـــا، النظرة المتكاملة التالية ضرورية.

تطوير سياسة:

مبادئ الأمن الموضوعية والرئيسية تزوّد a إطار للخطوة الحرجة الأولى لأيّ منظمة – تطوير a سياســة أمن. تمثّل سياسة أمن وجهة نظر المصرف العامّ إلى الأمن.

الأدوار والمسؤولية

إنّ ضابط معلومات المصرف الرئيسي (سي آي أو) يخصّص مسؤولية أساسية للتطوير، تطبيق، وصـــيانة البرنامج. لمساعدة، ضابط المعلومات الرئيسي قد يدعو لعقد a لجنة مـــدراء المصـــرف الآخـــرين مـــن الإنقسامات المختلفة أو أقسام المصرف. على الأقل سنويا، ضابط المعلومـــات الرئيســـي سيحضـــر إلـــى مجلس إدارة المنزلة العامّة للبرنامج. التقرير سيناقش أمور مادية تعلّقت بالبرنامج، عنونة قضـــايا مثـــل: تقدير الخطر؛ قرارات السيطرة وإدارة المخاطرة؛ ترتيبات مجهز خدمة؛ نتائج إختبار؛ إختراقات أمنيـــة أو إنتهاكات وردود الإدارة؛ وتوصيات للتغييرات في البرنامج.

تمييز الأخطار

الإدارة ستميّز التهديدات الداخلية والخارجية المنظورة إلى حدّ معقول التي يمكن أن تؤدّي إلـــى الكشـــف الغير مخوّل، سوء إستعمال، تعديل، أو دمار أنظمة المعلومات أو المعلومات. أبعد، إدارة ستطوّر وتطبّـــق الإجراءات والسيطرة الأخرى الذي يأخذان في الحسبان الإمكانية والضرر المحتمل هذه التهديدات.

الأخطار المديرة

الإدارة ستطوّر، يطبّق، وتبقي البرنامج للسيطرة على الأخطار المميّزة، متعـــادل بحسّاســـية المعلومـــات بالإضافة إلى التعقيد ومجال نشاطات المصرف.
الإدارة لها، إبتداء من اليوم، ميّز التدابير الأمنية التالية تخصّص للمصرف وأمّـــا لهـــا أو ســـتتّخذ تلـــك الإجراءات تلك الإدارة بعد قليل تستنتج ملائمة. إختبار الطرق يدرج أيضا [2].

غرض سيطرة / سياسة مصرف وصف أو إختبار إحالة إجراء
سيطرة على دخول على أنظمة معلومات الزبون تتضمّن السيطرة إلى: يحقّق ويسمح للوصول فقط إلى الأفراد والسيطرة المخوّلة لمنع مستخدمون من تزويد معلومات الزبون إلى الأفراد الغير مخوّلين الذين قد يريدون أن يحصلوا على هذه المعلومات خلال الوسائل المحتالة، سياسات المصرف التالية وضبط عنوان الإجراءات على الوصول: – بي سي / سياسة أمن شبكة إتصالات محلية – الإنترنت / سياسة إميل – سياسة برنامج حماية – إجراءات مدير أمن شبكة – تصرّف المستخدم والأخلاق للإستعمال الشخصي من مصادر المعلومات خارج مراجعة التدقيق القويّة السنوية للأمن والسيطرة الداخلية. الإختراق السنوي يختبر بالطرف الثالث، (يسمّيهم
يتضمّن تشفير معلومات الزبون الإلكترونية معلوماتا بينما في النقل أو في الخزن على الشبكات أو الأنظمة التي أفراد غير مخوّلين لربّما عندهم وصول. تزوّد المتابعة طرق تشفير معلومات الزبون الإلكترونية: تقنية في بي إن لإتصال الآمن إس إس إل تقنية للأعمال المصرفية على الإنترنت – بي جي بي وإجراءات كلمة سر للبريد الإلكتروني والإتصالات الداخلية أثناء السنويين خارج تدقيق مراجعة سيطرة التدقيق القوي، إرتباطات إس إس إل ستكون مجرّبة سويّة مع a مراجعة الرسائل البريدية الإلكترونية لإستعمال بي جي بي
أنظمة المراقبة والإجراءات لإكتشاف هجمات فعلية ومحاولة على أو تدخلات إلى الزبون / أنظمة معلومات مصرف – تقنية إن آي دي إس لإكتشاف التدخل يسجّلان المراجعات شهريا بتدقيق مدير أمن شبكة آي. إس . سيطرة ستراجع صفحة سجلّ مدير أمن الشبكة
برنامج الردّ الساقط الذي يحدّد الأعمال لكي تؤخذ متى المصرف يشكّ أو يكتشف بأنّ الأفراد الغير مخوّلين تمكّنوا من الدخول إلى أنظمة معلومات الزبون. محدّد في إجراءات سياسة الأمن، مدير أمن الشبكة سيجدّد إجراءات الردّ
يقيس الطوارئ والتغلب على آثار الكارثة للحماية ضدّ الدمار، خسارة، أو ضرر معلومات الزبون بسبب أخطار بيئية محتملة، مثل ضرر الماء والنار أو حالات الفشل التقنية – خطة إستمرارية عمل خطة تغلب على آثار الكارثة (أنظمة) بقابلية النظام المنسوخة. إختبار خطة التغلب على آثار الكارثة وخطة إستمرارية العمل سيؤدّيان ويوثّقان من قبل آي. إس . قسم على قاعدة سنوية

المراقبة: مراقبة الإجراءات من الضّروري أن تؤسّس لإكتشاف وضمان تصحيح الإختراقات الأمنية، مثل هذه التي كلّ الخروقات الفعلية والمشكوك فيها تميّز فورا، تحرّى، وتتصرّف بناء عليها، ولضمان الإلتزام المستمر بالسياسة، معايير، وممارسات أمن حدّ أدنى المقبولة.

الوعي، تدريب، وتعليم: وعي الحاجة لحماية المعلومات، يتدرّب في المهـــارات إحتـــاج لتشـــغيل أنظمـــة المعلومات بشكل آمن، وتعليم في التدابير الأمنية والممارسات من الأهمية الحرجة لنجـــاح برنـــامج أمـــن منظمة.

5.0 خاتمة

بالبيئة التقنية المتغيّرة باستمرار، الذي تعتبر أحدث اليوم ستكون ملغية غدا، وأمن يجب أن يماشـــي هـــذه التغييرات. أمن يجب أن يؤخذ بنظر الإعتبار كعنصر مكمّل ebanking. الأمن يجب أن يتعامل معه فـــي a proactive إسلوب لكي يتمكّن ه من أن يكون فعّال.

الإشارات

[1] "أعمال مصرفية آمنة على الإنترنت"، تي آر 401، لجنة أوروبية للأعمال المصرفية المعايير. مارس/آذار 1997، درب دي ترفويرين، 12, 1040، بروكسل.

إتش تي تي بي ://www.ecbs.org/ منشورات / أمن htm # دوستك 4

[2] "سياسة أمن معلومات"، www.bankersonline.com

[3] "أمن معلومات مدير"، معهد المدقّقين الداخليين،

إتش تي تي بي ://www.theiia.org/ecm/ تقنية cfm ?doc_id=849