BANKING, FINANCE AND INSURANCE COMMISSION

Annex to Circular CBFA_2009_17-1 of 07/04/2009

Sound practices for managing Internet security risks

Scope:

Credit institutions, insurance companies, investment firms and management companies of undertakings for collective investment and Belgian branches of these institutions which are governed by the law of a state that is not a member of the European Economic Area (EEA). The circular is also to be brought to the attention of institutions established in Belgium that are governed by the law of an EEA Member State.

1. Introduction

Financial institutions which provide services via the Internet face various security risks.

These sound practices therefore identify a number of specific attention points and recommendations with regard to the security of:

- an institution's own IT structure (hardware, operating systems, applications, databases, firewalls, email and web servers, etc.) against security threats associated with the Internet;
- financial transactions, consultations and management activities over the Internet.

Financial institutions are expected to comply with these sound practices or explain any deviations to the CBFA ("comply or explain").

2. Securing an institution's IT infrastructure

2.1. Rationale

All financial institutions that connect their IT infrastructure to the Internet need to take appropriate precautions to safeguard the security and continuity of their IT systems and the integrity and confidentiality of their financial and client information against any foreseeable abuse and risk arising from the Internet.

2.2. Prudential requirements

2.2.1. Security policy

Each institution that connects its IT infrastructure to the Internet must have an appropriate security policy in which attention is paid to:

- the need for appropriate security within the institution's own IT infrastructure and the objectives set out in this regard;
- the company's internal organization and responsibilities regarding:
  - monitoring threats to Internet security and checking them against the institution's security measures in respect of its own IT infrastructure;

  - protecting the internal IT infrastructure;
  - handling Internet security incidents;
- security guidelines for employees regarding safe use of the Internet;
- the security framework regarding the exchange of emails, files and messages (e.g. Instant Messaging) with people outside the institution;
- the policy and safeguards with respect to granting access to the institution's own IT infrastructure via the Internet (remote access);
- the appropriate criteria and responsibilities for periodically carrying out specialized security tests;
- the creation and storage of appropriate technical logs and their analysis, follow-up and reporting.

2.2.2. Analysis and monitoring of security threats and of the institution's security arrangements

The institution should provide:

- a solid analysis and monitoring of Internet security threats to its IT infrastructure, in light of the institution's security solutions and its Internet use;
- careful follow-up of published security gaps in the Internet infrastructure and security solutions used (software, hardware, programming languages, encryption, etc.). Where necessary, the institution should install as quickly as possible the corrective solutions provided by the supplier (software patches, upgrades, etc.) or use other solutions to cover the security risks.

Based on the analyses carried out and depending on the nature and scale of the identified Internet security threats, the institution should carry out periodic and formal risk assessments in order to determine whether and to what extent changes may be needed to the existing security measures, the technologies used and the procedures or services offered.

Depending on the urgency and seriousness of the findings, the conclusions drawn from the follow-ups and risk analyses should be submitted at least once a year to the senior management for approval.

2.2.3. Protection against unauthorized access or changes to the institution's IT infrastructure

Institutions should take the necessary security measures to avoid unauthorized access to and abuse of its IT infrastructure via the Internet.

To this end, institutions should use controlled bridges between the Internet and their own IT infrastructure, such as firewalls, proxy servers, mail relays, antivirus and content scanners or other similar security solutions. Institutions should ensure that these bridges are correctly designed, configured and secured and are under daily professional management and close monitoring.

In this regard, it is very important that all direct and indirect[1] links to the Internet flow via the aforementioned bridges. To guarantee that the resulting perimeter protection is watertight, institutions should also devote particular attention to preventing uncontrolled and inadequately secured network connections with the outside world (wireless networks, modems, etc.).

Since the aforementioned controlled bridges cannot (for the most part) check all information flows in an efficient and/or conclusive manner and where necessary stop all dangerous traffic, therefore institutions should also devote the attention necessary to adequate protection of the internal applications and databases that receive data or instructions via the Internet (principle of 'defence in-depth')[2].

2.2.4. Securing public websites

Public websites present an increased "security risk" because of the high number of visitors and easy access from the Internet. Institutions should therefore devote particular attention to securing their public

[1] In some cases, branch offices, agencies or subsidiaries linked to the institution's IT infrastructure also have Internet connections.

[2] 'Defence in depth' is a security strategy in which several lines of defence are placed in and around an object to be protected. A failure of one line of defence is therefore caught by the next line of defence.

websites, in order to make sure they are not subjected to unauthorized changes or used to distribute malware.

In order to limit the vulnerability of such websites and their servers, institutions should make use of:

- firewalls, proxy servers or other similar security solutions that protect the websites and their servers as much as possible against attackers or abuses via the Internet;
- security measures which strip the servers of all superfluous dangerous functions and protect ("harden") at-risk applications as much as possible. In order to enhance security even further, access by the various applications to the data and resources they need should be kept to a strict minimum (principle of "least privilege").

In order to prevent abuses committed using fake websites mimicking the legitimate sites of financial institutions, transactional and, preferably, purely informative websites as well must be identified by high-quality[3] digital certificates drawn up in the name of the financial institution or by other similar methods of authentication.

2.2.5. Authorized remote access to the institution's IT infrastructure via the Internet

The institution should adopt a policy regarding the access it grants to its IT infrastructure via the Internet, with particular attention to the rules regarding the granting, approval, monitoring, revocation and protection of such access.

Remote access should use high quality security solutions that:

- rely on strong authentication solutions that make it possible to determine with a high level of certainty the identity of the users who log on. A description of these authentication solutions is found under point 3.2.3.a.
- determine whether the actions by logged-in users are authorized;
- limit external access to the IT infrastructure to the strict minimum necessary (principle of "least privilege");
- provide for adequate security measures to avoid unauthorized access or changes to the institution's IT infrastructure resulting from security lacunae (viruses, malware, back doors, etc.) on the computer (infrastructure) of the users who log on to the system. Access to critical and sensitive components of the IT infrastructure should be possible, in principle, only by means of secured computers reserved for this purpose.

2.2.6. Security guidelines for employees

Operational management should approve the guidelines for employees regarding the secure use of the Internet and oversee compliance. Particular attention in this regard should be paid to:

- the risks posed by downloading and installing risky files;
- the precautionary measures relating to the use of email (suspicious emails, spam, etc.) and other Internet communication techniques (e.g. Instant Messaging);
- the precautionary measures and rules governing file transfers ((S)FTP[4], etc.);
- the risks relating to the often extensive Internet access and permissions of certain users or IT specialists.

Attentive to the problem of "phishing" emails[5] designed to mislead clients, and to the very low security level of email as regards the confidentiality and integrity of its content, institutions should develop guidelines on the acceptable use of email for commercial and other external contacts. These guidelines should also address other forms of Internet communication, such as Instant Messaging.

---

3 This involves "Extended Validation" SSL certificates with at least 128-bit encryption issued by recognized and generally accepted certificate authorities.

4 (Secured) File Transfer Protocol.

5 Fraudulent email messages that mimic legitimate emails in order to mislead the recipient and thereby to gain some advantage. In the financial world, phishing emails are often sent in order to obtain confidential credit card and/or bank card authentication data (usernames, passwords, etc.).

2.2.7. Incident management procedure

Institutions should have an incident management procedure in place to respond to Internet security incidents. Such a procedure should allocate the tasks/competencies in the event of serious Internet security incidents and set out the escalation process to be followed. The incident management procedure should also set out the tasks and responsibilities in respect of internal and external communication relating to major Internet security incidents.

2.2.8. Audit trails, analyses and reporting

In order to be able to track down, analyse and where necessary take steps against irregularities or attacks on Internet services, financial institutions should maintain the necessary technical logs and "audit trails" of access to and activities on its computer systems (including applications) and network components. These logs and audit trails must be adequately secured and stored in order to safeguard their integrity and evidentiary value. Ensuring their legal validity is an important consideration in this regard.

As a rule, the aforementioned logs and audit trails should be saved for a minimum of 6 months, so that they can be used in the event of a dispute or to analyse abuses.

Depending on the risk profile and scope of the Internet services offered, the institution should analyse, with suitable frequency, the logs and audit trails in order to identify irregularities or abuses. Each institution should ensure that it has the specialized resources and staff necessary for the purpose.

Any irregularities or abuses that have been identified should be reported through the appropriate channels to the senior management.

2.2.9. Independent security testing

Institutions which connect their IT infrastructure to the Internet should have an independent expert examine the Internet security measures that have been implemented. Such testing should include penetration tests and be carried out proactively before the institution's IT infrastructure or a new part thereof is connected to the Internet for the first time. The tests should be repeated thereafter as needed, depending on developments in terms of threats, usage or the significance of the changes to the existing Internet (security) infrastructure.

In general, these specialized tests ought to be carried out by independent external specialists who possess the requisite know-how, experience and resources. In exceptional cases, it may be acceptable for the institution to conduct the testing itself, provided it has the necessary expertise and that the person carrying out the test is not involved in any way in the development, implementation or operational management of the Internet services provided (e.g. in the internal IT audit).

3. Securing financial transactions over the Internet

3.1. **Rationale**

Financial institutions that allow their clients to consult or manage their data and/or to carry out transactions and/or submit them (in batches) via the Internet (hereafter referred to as "transactional services") are exposed to additional security risks, over and above the risks relating to the connection of the (internal) IT infrastructure to the Internet (cf. chapter 2).

Since financial institutions must have a connection between their own IT infrastructure and the Internet in order to conduct transactional services via the Internet, the following security requirements constitute a supplement to the security measures set out in Chapter 2.

Financial institutions which offer clients the option of using the institution's Internet security solutions and/or infrastructure to access Internet payment services provided by third parties (e.g. "3D secure" payments to online businesses) must take additional security measures (cf. point 3.2.8.).

3.2. **Prudential requirements**

3.2.1. Security policy

Institutions should ensure that their security policy pays due attention to:

- the need for appropriate security in the transactional Internet services offered, and the objectives set out in this regard;
- the internal organization and responsibilities with regard to:
  - monitoring Internet security threats relating to the transactional services offered;
  - the security of the transactional Internet services offered;
  - the centralization, handling and follow-up of security-related complaints, including client complaints;
- the protection and securing of both the client's and the financial institution's authentication data used in transactional Internet services;
- the protection and securing of the information exchanged and of client transactions conducted via the Internet;
- securing the transactional Internet applications used;
- communication with clients regarding the Internet services offered and the manner in which clients are advised to play their part in securing the Internet services offered;
- the creation and storage of appropriate technical logs and logical audit trails of Internet transactions, as well as their analysis, follow-up and reporting.

3.2.2. Analysis and monitoring of security threats and of the institution's security arrangements

Institutions should carry out a thorough analysis and monitoring of security threats relating to the transactional Internet services offered, taking into account the security solutions used by the institution and those offered to its clients. The analysis should cover both the security system as a whole and each individual component.

Based on the analyses carried out, and taking account of the nature and scale of the Internet services provided, institutions should carry out a formal risk assessment at least once a year, in order to determine whether and to what extent changes may be needed to the existing security measures and to the technologies and procedures used. These assessments should also take into account the time needed to implement the necessary changes (including client roll-out) and the anticipated developments in security threats during that period.

Depending on the urgency and significance of the findings, the conclusions drawn from the follow-ups and risk analyses should be submitted at least once a year to the senior management for approval.

3.2.3. Securing the authentication process

It is crucial that every access to and use of the Internet services offered be legitimate. Institutions should therefore use strong authentication solutions that are well suited to the nature and the risks of the Internet services provided and that allow for a very high level of certainty in verifying the identity of the users who log in.

In choosing an authentication solution, institutions should take into account the client-side Internet security risks and the possibility for clients to assess and cover these risks.

a) Authentication solutions for private individuals

In the aforementioned context, and given the significant increase in threats from

- phishing attacks,
- fake websites,

- the increased spread of malware on client computers that try to steal a variety of confidential data such as authentication (e.g. usernames, passwords) and financial information (credit card information, etc.),

authentication solutions that rely exclusively on a limited number of reusable secrets (e.g. username and password, whether or not in combination with personal TAN cards[6] or series of numbers or private software PKI keys[7], etc.), which can surreptitiously be stolen via the Internet, are no longer acceptable for use with fraud-sensitive Internet services. For Internet services that are purely consultative in nature, institutions should carry out a sensitivity analysis and set out an appropriate confidentiality and security policy. When using a one-time password for authentication, institutions must also ensure that the validity period of such passwords is limited to the strict minimum (i.e. maximum a few minutes).

b) Authentication solutions for companies and professionals

For transactional Internet services intended for companies or professionals, institutions can use appropriate authentication solutions in which the counterparty is wholly or partly responsible for securing its personal authentication data as well as the hardware and software within its own IT infrastructure. In that case, the companies and/or professional counterparties are informed by the institution as to the expectations regarding their internal security measures, and the responsibilities in this regard should be clearly outlined in the relevant contracts.

c) Internal security measures

Institutions should see to it that all authentication data required by their clients and all client-oriented hardware and software are delivered to their clients by secure means. Software that is made available to a client and that must be used by that client should be physically delivered and/or digitally signed by the financial institution in order to enable the client to verify its authenticity.

In order to allow users to identify an institution's transactional website, the institution should use high-quality digital certificates[8] identifying it by its name, or other equivalent authentication mechanisms.

Institutions should ensure that all data or files used to identify their clients and their own websites are appropriately secured against theft or unauthorized access or modification.

Institutions should limit the maximum number of failed login attempts after which access to the Internet service is (temporarily or permanently) blocked, and should also limit the maximum period after which inactive Internet sessions are automatically terminated (as a rule, maximum 15 minutes). Institutions should have a secure procedure to reactivate blocked Internet services.

3.2.4. Protecting and securing transactions

In order to safeguard the confidentiality of transactions and information exchange between a client's computer and his or her financial institution, institutions should use strong and widely recognized encryption techniques.

The institution should have in place technical procedures for verifying authentication (e.g. Message Authentication Codes [MACs], etc.), in order to detect accidental changes in client transactions resulting from technical malfunctions.

In addition, institutions should have adequate security and/or monitoring solutions which make it highly probable that fraudulent transactions can be prevented or detected before they are carried out. Examples of effective security solutions include one-time passwords or electronic signatures generated with key characteristics of the client transaction (e.g. amount and/or part of the beneficiary's account number) or

---

6 Cards or other sources of data with a limited number of previously generated passwords that the client must enter when logging on or carrying out transactions. In such cases, the Internet application indicates which password the client should enter.

7 For the purposes of a software PKI (Public Key Infrastructure), each user is identified separately by means of a private software key which he or she has been issued and which is often stored on the client's computer.

8 Extended Validation SSL certificates with at least 128-bit encryption issued by recognized and generally accepted certification authorities.

qualitative dual-channel solutions[9], whereby the client's Internet transaction is confirmed via a second, independent communication channel (e.g. via mobile phone). In the case of Internet services provided to companies and/or professionals, moreover, use is often made of the separation of functions built into the Internet application, whereby a transaction must be entered and/or approved by several persons (principle of "independent checker or validator").

Institutions should verify in an appropriate manner, depending on the nature and risk level of the transaction, the identity and associated authority of the client for each client transaction[10] that it receives.

3.2.5. Securing Internet applications and servers

In developing and maintaining Internet applications, Institutions should pay due attention to:

- the security characteristics and risks of the application architecture, programming techniques and routines used, in order to limit as much as possible the application's vulnerability to malicious attacks (e.g. session hijacking, SQL injection, cross-site scripting, buffer overflows, etc.).
- the consequences of its technology choices for the security on the client-side (e.g. use of multimedia applications, plug-ins, external links, etc.).

In this regard, it is important that both the developers of the applications and the managers of the controlled bridges between the Internet and the internal IT infrastructure (cf. point 2.2.3) have sufficient knowledge of the organization and the operation of the various lines of defence ('defence in depth') [11] and of the interaction between them.

Moreover, the protection of transactional websites and servers should meet the same standards as those of public websites (cf. point 2.2.4.).

3.2.6. Communicating with the client

Although the use of technological solutions is necessary in order to protect financial services via the Internet, these for the most part are not in themselves sufficient guarantees of security. The use of the technologies and applications made available to the client, as well as the client's own efforts to ensure the security of his or her own computer (infrastructure), often constitute the weakest links in the security chain.

Institutions should provide simple, comprehensible manuals and documentation on this subject to inform clients of their responsibilities with regard to the secure use of the Internet services provided.

The following aspects must, at the very least, be mentioned in such documentation:

- the client's obligation to keep the secret authentication or PIN codes confidential;
- the rules with regard to the proper and secure use of all the hardware and software used by the client (client's own computer, etc.);
- the procedures to follow in case of loss or theft of the confidential user information or client-specific hardware and software needed to log in or to carry out transactions,
- the procedures to follow if an abuse is detected or suspected;
- the policy of the institution regarding sending email or other electronic messages (e.g. Instant Messaging, SMS, etc.) to clients.

The institution should also have a suitable communication policy to inform and/or make clients aware in a timely manner of new developments and matters requiring attention with regard to the safe use by the client of the Internet services offered.

---

9 Dual-channel solutions in which the second communication channel used is not exposed to the same risks as the first channel. Since more and more communication channels are connected to the Internet and use Internet technologies, the independence of the 2 channels used must be re-evaluated at least once a year.

10 The bundling of several similar client transactions is permitted inasmuch as this does not endanger the requisite high security of the transactions.

11 'Defence in depth' is a security strategy in which several lines of defence are placed in and around an object to be protected. A failure of one line of defence is therefore caught by the next line of defence.

3.2.7. Independent security testing

Institutions that use the Internet for transactional purposes (e.g. concluding an insurance policy, transmitting payment instructions and/or stock exchange transactions, etc.), and/or to enable clients to consult confidential data, should have an independent expert test the security of their transactional Internet services before launching the Internet services in question. This should then be followed by independent specialized security tests as needed, depending on developments with regard to threats or any technical or functional changes to the Internet services offered. The tests conducted should include both penetration[12] and application tests[13] for various sorts of online attacks.

The requirements as regards the expertise and independence of the experts used are the same as those in point 2.2.9.

3.2.8. Participation in Internet payment services provided by third parties

A financial institution that offers clients the option of using that institution's Internet security solutions and/or infrastructure to access Internet payment services provided by third parties (e.g. "3D-secure" payments) must develop an acceptance policy in this regard, which takes into account:

- the reputation and the financial and operational solidity of the provider of the Internet payment services;
- the nature and risks of all aspects of the payment services offered (amounts, beneficiaries, etc.), taking into account the security solutions and/or options offered;
- the demarcation of the parties' responsibilities with respect to securing the transactions and compensating clients in the event of abuses and/or disputes;
- the legal (control) status of the provider of the Internet payment services;
- potential reputation risks to the financial institution.

Senior management (usually the management committee) should approve the acceptance policy and oversee compliance. Institutions should annually conduct a thorough analysis and follow-up of identified threats to the accepted Internet payment services, in light of the security solutions in use.

[12] In a penetration test, the security of the perimeter of the institution's own IT infrastructure should be verified.

[13] E.g. "application cracking", in order to check whether the application is vulnerable to attacks such as SQL injections, cross-site scripting, buffer overflows, etc.