



**Recommendation No. 1 of 2009 (10 February) of the
Board of the Hungarian Financial Supervisory Authority**

On internet security risks

I

The Goal and the Scope of this Recommendation

Noticeable over the years, financial services provided over the Internet have become ever more dynamically widespread worldwide, and thus also in Hungary. This is obviously due to the fact, that internet-based financial services are more cost efficient and more comfortable for both the service providers and their customers.

However, the more transactions and the greater turnover that is attracted by the internet channel, the more attractive it becomes for well-organised, technically qualified, multinational criminal circles.

The HFSA has conducted surveys in connection with this process and has consulted its supervised institutions, as well as its sister authorities. The surveys have shown that financial organisations offering services over the internet were not sufficiently prepared for internet-based threats. The Board of the Hungarian Financial Supervisory Authority therefore deems it necessary to formulate a recommendation to set forth its expectations with regard to this topic.

Based on the above, the objectives of this Recommendation are as follows:

- To facilitate the uniform interpretation of the concepts and requirements related to internet security and to facilitate compliance by market participants with the statutory obligations related to the objective, technical and information technology conditions that are necessary for the secure functioning of financial organisations, in order to avoid threats to secure transactions over the internet and thus to avoid threats to confidence in the financial markets;
- To contribute to an awareness of the internet security risks of financial organisations and to help contain those at a manageable level, in order to prevent the internet security threats directed at the sector and to manage those in a regulated and optimal way.

This Recommendation is addressed to financial organisations that provide or are planning to provide services that can be used (also) over the internet.

The legal provisions governing this Recommendation are as follows:

- Act CXII of 1996 on credit institutions and financial enterprises (the Credit Market Act – CMA), with particular consideration to Articles 13 (personal and objective conditions) and 13/B (on the security of information technology systems);
- Article 44 (personal and objective conditions) of Act LXXXII of 1997 on private pension and private pension funds (the Private Pension Act – PPA);
- Article 40/C/2 (protection of information technology systems) of Act XCVI of 1993 on voluntary mutual insurance funds (the Voluntary Fund Act – VFA);
- Article 65/b of Act LX of 2003 on insurance companies and insurance activities (the Insurance Act – IA);

- Act CXXXVIII of 2007 on investment firms and commodity dealers and on the regulations governing their activities (the Investment Enterprises Act – IEA);
- Article 7 (protection of information technology systems) of Government Decree 283 of 2001 (26 December) on the required personal, objective, technical and security conditions for investment and commodity dealership services, the safe-keeping of securities, custodial services and for clearing house activities;
- Act XXV of 2005 on telesales.

This Recommendation will not repeat any statutory provisions or any other issued supervisory recommendations. Should statutory regulations prescribe requirements that extend beyond this Recommendation, then the HFSA will demand compliance with those.

By occasionally indicating expressions (also) in the English language in this Recommendation, the HFSA strives for the accepted international terminologies to be conveyed to financial organisations in Hungary as accurately as possible with regard to their substance.

II Preamble

1. In order to comply with the statutory obligations and to preserve the confidence in the system of financial intermediaries, the HFSA expects financial institutions to establish optimal internet security.
2. In connection with the above, it is a fundamental requirement for financial organisations to operate their information technology systems securely, based on “Methodological Guidance No. 1 of 2007 of the Hungarian Financial Supervisory Authority on the protection of the information technology systems of financial organisations”.

III Expectations in relation to the internet security of financial organisations

3. The HFSA expects financial organisations to regularly, but at least once every two years, conduct an internal survey of their internet security risks, in which they should specify the following:
 - Classification into **protection** security classes, by surveying and selecting the objects and operating processes (*information technology systems, applications, completed systems, databases, business processes, etc.*), they need to provide internet security protection for in some way;
 - The internet security threats to the elements classified into the protection security classes and the effects of the potential damages on the institution and on the customer;
 - The quantified risks (loss and frequency) of the selected elements and their threat levels. The threat-object pairs should be assigned security risks, with the expectation that the methodology should be documented, without prescribing the methodological depth. It is widespread to use the loss value multiplied with the occurrence frequency for quantification, but it is expedient to use a more refined approach for the internet security risks of financial organisations.
 - **Risk management**, by assessing the individual internet security risks as acceptable or to be mitigated. For risks to be mitigated risk management should specify the measures to be used for mitigating the given risk to an acceptable level.

- **Financial organisations** should organically integrate **this survey** into their operational risk surveys performed every year, and should consider it when specifying their capital requirements for operational risk and when conducting maintenance on their policy, procedural rules and protective measures. The quantification of internet security risks is part of an institutional procedure aimed at the quantification of a larger unit, that of operational risks.
4. The HFSA recommends that financial organisations should specify within their regulations and procedures the activities and functions that they rate as highly risky with respect to internet security, for which therefore they wish to perform the risk assessment at shorter intervals than every two years.
 5. Following the assessment and management of the risks, financial organisations should, if necessary, update their security concept to contain the following:
 - Security strategy: goals, basic principles, liability limits;
 - Actual status (the results of the risk analysis);
 - Specification of necessary measures;
 - Execution schedule for the necessary measures with deadlines;
 - Analysis of the interaction of the measures.
 6. The HFSA expects financial organisation providing online services to have procedures related to internet security. The internet security policy should regulate, among others, the means and the technical conditions for continuous and extraordinary contacts with customers. It is important for the procedures, and in particular for the incident management plan, to be updated in addition to the prescribed frequency, in case of an incident, out of turn if necessary.
 7. In connection with internet security procedures, organisations are expected to constantly follow the minimum standards and best practice procedures, the expected threats and the related risk typology as published in the international professional literature, and if necessary, to update their risk analyses accordingly. Subsequent upon to constantly monitoring and analysing the environmental changes, the changing threats and risks are to be re-assessed to enable the enforcement of justified changes within prevention, defence, procedures and in training.
 8. Furthermore, it is necessary for the realisation of internet security and for the organisational unit involved in its implementation to be organically integrated into the financial organisation's security organisation, where they should be represented by dedicated and qualified professionals with appropriate responsibilities and decision making powers.
 9. The HFSA expects financial organisations providing online services to have a monitoring strategy for their internet-based business activities and for the corresponding internet security. The strategy should contain the automated workflows for the detection of unusual activities and for the appropriate alerting procedure.
 10. The HFSA considers it practical for financial organisations providing online services to address their internet security risks along accurately and clearly defined liability principles within their internal regulations for internet-based services and within the contracts required for their use.
 11. Of the employees of financial organisations providing online services, it is recommended that those involved in the provision of the service should be provided training and extension training customised to their roles. It is an indispensable part of the training to present how

regulations related to internet security can be implemented in everyday practice. Staff should receive regular briefings on changes that impact the environment, the regulations and the procedures.

12. With regard to training, the HFSA expects that there should be a detailed training concept in relation to internet security, separately for certain selected professionals, separately for bank clerks and separately for customers. The concept should contain the following:
 - The target groups;
 - The training syllabuses for the target groups;
 - The qualifications of the professionals directing and providing the training sessions;
 - The time-tables for the training sessions, including those for extension training;
 - The life cycle of the concept and of its individual elements, and the required updates;
 - The measurement of the efficiency of the training sessions.
13. The HFSA recommends that financial organisations should regularly (even once every year, if necessary) have independent external audits made of their internet security. On the basis of this they should record the risks related to internet security within the operational risks of the financial institution, to enable risk management to be developed in time.
14. It is expected of the audits to be directed by professionals with practice and experience in the internet-based business lines of financial organisations, in order to enable also the discovery of internal vulnerabilities. In addition, it is practical for them to have references also within the area of internet security, to be able to specify the internet-specific parameters of the audit and to be able to analyse the results on the basis of an appropriate knowledge of the subject matter.

IV

Internet security expectations related to the services of financial organisations provided over the internet

15. The HFSA expects financial organisations to ensure that their services provided over the internet are seamlessly integrated into their organisational hierarchies, with unambiguous decision making, competency and liabilities.
16. The internet is an open, global network that is essentially not secure. Financial organisations must be prepared for the risks and for the management of ever more dangerous security threats. Due to all of this it is indispensable for financial organisations to implement strong security measures and controls in proportion to the threats and risks involved.
17. Financial organisations must warrant the authentic and satisfactory security of the identification of their customers who log on over the internet and of the transactions conducted over the internet. This requires as a condition the realisation of controls and the development of a security strategy that should fully accomplish the following objectives:
 - The confidentiality of data;
 - The invulnerability of the system;
 - The availability of the system;
 - The authenticity of customers and transactions;
 - The protection of customers and their identifiers.
18. The HFSA expects confidential data to be accessible only to people with access rights of an appropriate level. It is practical for financial organisations to use such encryption within their online systems which is required and sufficient on the basis of the operational and network risks.

19. This Recommendation does not specify the type or the strength of the encryption to be used, but it expects financial organisations to regularly evaluate the security requirements of their internet-based applications and to employ encryption that is in proportion to the level of invulnerability and confidentiality that is required, and that complies with the international norms and standards.
20. In accordance with the general principles of data protection, it is recommended that the security of the customer's PIN code and of his other similarly sensitive details be managed end-to-end at the application layer. This represents the requirement that the encryption process should remain intact and unscathed from the point of arrival of the data to its final destination, where decryption and authentication take place.
21. The invulnerability of the system refers to the accuracy, reliability and full completeness of the flow, storage and processing of information between the customer and the financial organisation.
22. Financial organisations are recommended to install monitoring and surveillance systems that raise alerts in the case of irregular activities or unusual transactions.
23. Online services (provided over the internet) must have a high level of availability in order to gain and retain the confidence of customers. All security measures are in vain, if the system is not available when customers need it. Customers expect online services provided by financial organisations to be available nearly 24 hours per day, every day of the year, i.e., with almost zero system downtime, and that the corresponding service level be declared and ensured for the connection between the institution and the customer.
24. The following are important factors for a high level of system availability: sufficient capacity for concurrent user requirements (with continuous monitoring and expansion if necessary), reliable performance, quick response times, scalability, and the ability to quickly recover from an error.
25. Back-office systems are just as important to online services as the system ensuring the internet-based connection. Availability also relates to the back-office systems that are required to serve customers and to the related backup solutions as set forth in the business continuity plan (such as the use of facsimile machines by investment enterprises offering online services in cases of service outages).
26. In addition to the logs for business purposes, financial organisations are expected to continuously monitor the performance of their systems, their server processes, the extent of their traffic, the transaction times and the utilisation of their capacities using appropriate monitoring tools, to be able to ensure minimum interruptions to the availability of their online services.
27. With regard to the authenticity of customers and transactions it is practical to consider the following:
 - a) Data flows in both directions in an online connection conducted over the internet between a financial organisation and its customer. When talking about a transaction, either of the parties may serve as the initiator or as the destination. Thus, transaction authenticity is an expectation in both directions;
 - b) With regard to the integrity of the flow of data, the invulnerability of the information within the initiation of a funds transfer by a customer is just as important as the authenticity of the confirmation sent as a response by the financial organisation;

- c) Financial organisations should also verify whether or not an identified customer is authorised (under a contract or under the business regulations) to perform the transaction that was initiated.
28. When identifying a customer, the financial organisation is responsible for verifying whether or not the person logging in is identical to the person registered in the records of the financial organisation with the specified access rights. Of the various pieces of information that can be used for identification, multi-factor identification requires the use of at least two of the following:
- Something known by the customer (password, PIN code, other personal details, etc.);
 - Something the customer possesses (token, smart card, cellular phone, etc.);
 - The customer himself/herself (fingerprint, facial image, etc.).
29. The HFSA expects financial organisations to use a two-factor identification procedure by all means within their interactive and transaction-based connections for their services provided over the internet, due to the risk levels.
30. It is reasonable to demand again the second level of the two-factor identification procedure for transactions of a higher value or when sensitive customer details are modified.
31. Transaction content integrity is the requirement to ensure and to verify whether or not a transaction may have been modified while being transmitted. It is expected that an authenticated and encrypted connection should remain fully intact for the whole duration. In case of any interference the connection should be interrupted leaving the affected transactions suspended and informing the customer as soon as possible using some other channel (email or telephone). The transaction data are to be retained in an invulnerable form.
32. As proof of transaction origin retained transaction messages should contain data or information that could only originate from the authorised initiator of the transaction. The HFSA draws attention to the fact that ensuring that a transaction's origin cannot be denied does not yet in itself ensure the full protection of the transaction.
33. A receipt that can not be gainsaid ensures protection for the initiator of the transaction in case it may not be possible to verify the transaction in the destination system. The addressee returns a confirmation message to the initiator. The message should contain information that could only originate from the original transaction message. Simple serial numbering is not sufficient. According to the practice considered by the HFSA as good practice, the message for receipt confirmation should also be authenticated and the integrity of its content should be verified.
34. The sequential ordering of transaction messages protects the addressee against their loss or their deceptive copying. This is also a statutory obligation for some financial organisations (such as investment enterprises providing online services).
35. The protection of the customer's interests and personal details is of fundamental importance to financial organisations when providing services over the internet. In recent years there has been a proliferation of targeted attacks with the goal to obtain the personal data of customers that could be used for identification. Using techniques based on mutual agreement customers may also verify the veracity of the financial organisation in an online connection. Such methods could include the following: selection of defined, personalised messages or images, or secret questions and answers based on pre-recorded information, etc. In an SSL connection the customer may inspect the security certificate of the financial organisation's web-site. In connection with the above, financial organisations are expected to supplement two-factor identification within the process in transaction-based customer relationships, as an organic

part thereof and as necessary, with security elements that minimise the risk of man-in-the-middle (man-in-the-browser, man-in-the-application) type attacks.

36. An interactive connection conducted over the internet between a financial organisation and its customer can be broken down into three locations with regard to internet security:
 - a) The system of applications developed for this purpose by the financial organisation's information technology division:
 - Point of entry (mostly the web interface of the institution);
 - Applications performing customer identification and access control;
 - An application accepting customer information and requests;
 - An application that obtains the responses, that establishes contact to the institution's other systems;
 - Transmission of responses to the customer;
 - Ensuring the integrity, verification, encryption, etc., of the questions and answers;
 - Applications that monitor and log the process (to enable retrieval).
 - b) Applications used by customers:
 - Computer with an operating system;
 - Browser;
 - Security applications (antivirus, firewall, antispymware, etc.);
 - Device required for identification (token, cellular phone, etc.).
 - c) The internet channel that connects the customer with the financial institution:
 - Interface established over the browser;
 - The possibility of an interactive connection;
 - Ensuring the bi-directional flow of data;
 - Encrypted (SSL) communication channel.
37. The HFSA considers an interactive internet-based connection between a customer and the financial organisation to be secure, if the identification of the user is beyond doubt, and if the bi-directional flow of information during the interactive online communication meets the principles of full integrity of content, data security, continuous authenticity and irrevocability.
38. It is the financial organisation that encourages its customers to use the internet channel; it is therefore the responsibility of the financial organisation to ensure its secure use for its customers. Thus it is expected of the financial organisation to use its best efforts to provide for security on the side of the financial organisation as well as for the internet channel (with consideration to the international practice, using methods relying on risk analysis, etc.), and to inform the customer of the security requirements that it expects the customer to implement.
39. It is unreasonable and disproportionate to require customers (be it set forth in the service agreement) to accept restrictions for the sake of security which are too complicated for them, or which are prohibitively uncomfortable, and/or demand excessive financial sacrifices, because comfort, simplicity and cost-efficiency are exactly the real attractions of services provided over the internet.
40. At the same time it is exceptionally important to provide a broad range of information to customers, to assist them in obtaining the appropriate information and guidance, because the more fully they understand the prescribed security measures, the more likely they will be to observe them and the more confidence they will have in the online services of the financial organisation.

Closing Provisions

41. This Recommendation is a legal instrument issued pursuant to Article 12 (1) d) of Act CXXXV of 2007 on the Hungarian Financial Supervisory Authority, and its provisions shall extend not only to the service providers already active, but also to service providers that will enter the market later.
42. The substance of this Recommendation, issued by the Board of the HFSA, expresses the requirements as set forth in the statutory regulations, the principles and methods recommended for implementation on the basis of the law enforcement practice of the HFSA, as well as the market standards and the usual market practices. The HFSA shall verify whether or not the provisions contained in the regulations of the financial organisation comply with this Recommendation and shall compare the relevant practices of the service providers. In case of a deviation in practice it will call upon the service provider to develop regulations that correspond to this Recommendation.

The propagation of financial services provided over the internet

- 1 Noticeable over the years, financial services provided over the Internet have become ever more dynamically widespread worldwide, and thus also in Hungary. This is obviously due to the fact, that internet-based financial services are more cost efficient and more comfortable for both the service providers and their customers. In the recent years internet-based services have developed into successful service lines in insurance, on the capital market, in investment services and in banking: according to a survey conducted by the GKI Economics Research Corporation and Sun Microsystems the number of customers who had contracts for internet banking services was nearly 2 million in 2008 (of which 1.7 million were retail and 270 thousand were corporate customers).
- 2 However, the more transactions and the greater turnover are attracted by the internet channel, the more attractive it becomes for well-organised, technically qualified, multinational criminal circles. Of the IT-security professionals working in the international financial sector, 80% are seriously concerned about malware being used to steal our sensitive business information (Finjan Web Security Survey 2008). In the United Kingdom for instance, the direct losses caused by phishing already amounted to GBP 33.5 million in 2006, against a backdrop of GBP 12.2 million in 2004, while the number of phishing attacks has grown from 2,369 attacks per quarter to 10,235 attacks per quarter (APACS 2008).
- 3 This international process has now reached Hungary as well.
- 4 There will be an even more dynamic growth in the widespread use of the internet in Hungary in the future.
- 5 The internet penetration at Hungarian public institutions has reached 97% (BellResearch), and thus the use of the internet to manage affairs is becoming increasingly acceptable and accepted.
- 6 According to data from the Information Society Research Institute (ITTK) for 2006, 90 percent of young Hungarians between 14 and 17 years of age are already active users of the world wide net.
- 7 According to the research about the habits and values of young Hungarians, 67 percent of young Hungarians between 14 and 17 years of age use the internet daily, while 21 percent use it several times a week. Of every ten teenagers seven are members of some community site.
- 8 This data projects an increasing demand for the internet-based services of financial organisations.
- 9 International analyses indicate that the commitment of the supervised sectors to offer internet-based services is increasingly becoming a business necessity demanded by the competition in the marketplace.
- 10 There are by now more than 11 million different types of malware in the world, and every 5 seconds a new web page is infected with malicious intent (Sophos, July 2008).

- 11 Consequently, in the future the HFSA and the financial organisations will encounter an increasing number of exploitation attempts on the internet in Hungary, too, with increasing threat levels.

Services provided by financial organisations over the internet

Distinctive features of online services (provided over the internet)

- 1 As a consequence of the open and dynamic nature of the internet, online services are essentially more risky than those using closed networks and dedicated channels.
- 2 Due to the enhanced risk situation, special controls and security procedures must be developed to manage the risks of online services. Financial organisations assign security levels and measures to their various internet-based services that correspond to the given service.
- 3 The extent of the risk is not independent of the type of the online service. With respect to risk, online services are categorized into three categories: services providing only information (unidirectional and static), interactive exchange of information and transaction services.

Types of online services

Services providing only information

- 4 Unidirectional communication is the most fundamental type of online service, conveying information, advertising, campaigns, etc., to the customer.
- 5 The related risks were not significant for a long time, damages to the conveyed information represented reputational risk to the financial organisation at most.
- 6 The new attack strategies however, including access to the computers of visitors using poisoned internet pages to infect them, justify the enhanced, strict protection of the web pages of financial organisations. Financial organisations, as publishers responsible for providing information, should ensure that their own homepages are impossible to forge, with particular regard to the fact that their customers generally use this route to access their online services.

Services providing for the interactive exchange of information

- 7 These services are more risky than the previous, regarding the fact that here customers take the initiative in communicating with the institution, asking questions, completing requisition forms, querying balances, etc.
- 8 The extent of the risk depends on the type of the application used by the customer, and on the form and depth that the information sent by the customer is received by the information technology system of the financial organisation.
- 9 It is a non-negligible risk that such types of services require the identification of the customer, and the protection of the extremely sensitive customer details used for the identification is part of the risk.

Services that also provide facilities for transactions

- 10 These services enable customers to issue orders for financial transactions online, such as for funds transfers, for fee payments, to fix deposits, etc.
- 11 This is the most risky type of online services, because financial orders thus issued are executed rapidly, automatically, and mostly irrevocably.
- 12 The entire system may become exposed, if the security controls are not adequate.
- 13 The risk is amplified as an attack on the system does not require personal or physical presence, it can be executed even from another end of the world.
- 14 It is a distinctive feature of the risk that the attack occurs quickly, over a short period of time, is mostly impossible to recognise in real time, and it is also not easy to establish who made the attack, with what method and from where.

Internet security threats posing dangers to the services of financial organisations provided over the internet

In May 2007 the European Commission issued a communiqué on “Defining the European Commission’s global policy on the fight against cyber crime”. Within its communiqué the Commission stated that there was not even an accepted conceptual definition for cyber crime, and recommended a definition consisting of the following three points:

- 1 Traditional forms of crime, such as fraud and forgery, committed over electronic communications channels and information systems.
- 2 Publication of illegal content over electronic media (i.a. child sexual abuse materials or incitement for racial hatred).
- 3 Crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking.

In the same paper the Commission defined eight problem areas:

1. A growing vulnerability to cyber crime risks for society, business and citizens
2. An increased frequency and sophistication of cyber crime offences
3. A lack of a coherent EU-level policy and legislation for the fight against cyber crime
4. Specific difficulties in operational law enforcement cooperation regarding cyber crime, due to the cross-border character of this type of crime, the potential great distance between the crime perpetrator and the crime victim and the extreme speed with which crimes can be committed
5. A need to develop competence and technical tools (training and research)
6. The lack of a functional structure for cooperation between important stakeholders in the public and the private sector
7. Unclear system of responsibilities and liabilities for the security of applications as well as for computer soft- and hardware
8. The lack of awareness among consumers and others of the risks emanating from cyber crime

We have entered a new era with regard to the risks threatening the security of the internet:

- In 2007 the market for illegally obtained personal data in the United States was on par with the market for drugs and the market for prostitution with regard to their traded values;
- In order to exploit the possibilities in this market, several well-capitalised and technically equipped international organised criminal networks have been established, modelled after multinational corporations;
- Their organisational hierarchies and geographically diversified distribution of work is a perfect implementation of modern corporate structuring principles and they also efficiently conceal the established criminal network from the law enforcement organisations.

The emergence of organised criminal networks has completely changed the methodology and the process by which cyber crime is perpetrated.

- 1 In their distribution of work the first group obtains the internet banking passwords (or the bank card details, together with PIN codes) and sells them over the internet to anonymous data brokers. Those re-circulate the data to cashiers, who perform the wizardry to turn the data into cash. There is also a distribution of work in laundering the money. Spammers recruit money mules, to receive bank transfers using their bank accounts (mostly duped as naïve buffs) and to withdraw the cash and send it on to third countries with the use of cash forwarding businesses (such as Western Union).
- 2 Most recently the acquisition of internet banking passwords also takes place in a distribution of work. Phishermen operate web pages that look like real pages of banks, with spammer networks directing customers to these pages. Both the phishermen and the spammer networks hire malware writer teams that provide them with complex hacking tools and kits that are capable of compromising the computers of millions of innocent computer owners to use them for their own purposes (botnets).
- 3 A new profession has also emerged, that of the botnet herder, who manages millions of compromised computers (zombies) and leases them to spammer networks or phishermen. In addition to this, botnets can be used for real cyber attacks, a company, an industry or even an entire country (such as an online betting office, or CNN, or Estonia) can be blackmailed by paralysing its internet traffic. This is also a threat to financial organisations.
- 4 Hacking has become a flowering industry and its tool-sets have flooded the market as mass products. The use of crimeware no longer requires any special skills, whoever buys them can start using them immediately, like any other common program, relying on user instructions, help, FAQ (Frequently Asked Questions) and online support (web-based help). There are keylogger spyware programs, data acquisition and forwarding programs and phishing page editors that can be leased or purchased on the internet and can be used with a simple graphical user interface, just like other customary image or text editors.
- 5 The quality of the programs that can be obtained is increasingly good; developers support their products with serious investments, real research, development and testing and customer service. Most tools are developed with an understanding of anti-virus software and thus the mutant malware is not recognised by the anti-virus software. By the time anti-virus software is updated, the malware already appears in newer versions. This is an accelerating arms race between the offensive and defensive online armies.
- 6 The most frequent form of crimeware testing is to send tricky email attachments and to use infected, poisoned web pages. Organised crime however also creates its own market economy. For example, in the framework of an “affiliate marketing program” it incentivises webmasters to install malware on their web pages. Webmasters receive commissions (of USD 0.08-0.50) for each infected computer, if the malware was downloaded from their page by the unsuspecting innocent user.
- 7 Collective Internet Attacks (CIA, as referred to by information technology professionals with a sense of humour) are the next step in the arms race. Here SQL injections, Web-based Exploits, Botnet tactics and malware are used to launch an all-out assault to compromise the computers of unsuspecting and mostly unwary users, to gain control and power over their machines, and to acquire data that can be sold on the market.
- 8 We could witness the first attacks of this kind in the first half of 2008, when within a few days more than a quarter million web pages were poisoned, including the pages of businesses, shopping centres, schools, the media and municipal institutions.

- 9 The most frightening in all of this, is that simple users do not notice any of this. They do not even suspect that their computer may already be a botnet zombie, controlled by someone else.
- 10 Protection against malware is based on a characteristic code (its signature) that can be screened out from its instruction lines, which is as if it was the signature of the program. When anti-virus software finds a new virus or spyware, it searches for this signature, and in possession of this signature it can recognize and screen the malware at any later point in time should it reappear.
- 11 If however, it cannot find the signature in its list of malware, it will not be able to recognise the intruder as a prohibited program and will allow it to be installed on the computer.
- 12 Cyber criminals garble the computer code and fill it up with nonsensical lines to prevent the recognition of their malware, thus confusing the anti-virus software that tries to identify the malware (code obfuscation). Not finding the concealed signature, the anti-virus software considers the malware as harmless.
- 13 Cyber criminals have even further improved on this technique. They take the garbled code and use refined encryption methods to render it indecipherable. The decryption key necessary for the execution of the code is received by the malware over the internet from a remote server.
- 14 Anti-virus applications based on behavioural patterns have shown, that 80% of all malware works with garbled code, and that usual anti-virus and anti-intrusion programs are not capable of recognising those.
- 15 Cyber criminals conceal the newer versions of these encrypted malware programs in seemingly harmless PDF and Flash files. One such PDF file was examined by all anti-virus programs, of which only 10% suspected the file to be dangerous.
- 16 Targeted “man-in-the-middle” type attacks have already appeared as live threats, projecting the risks of the future.

Cyber criminals find ever newer assault techniques in this escalating arms race. One of the extremely effective old-new methods is to exploit and to manipulate the natural tendency of humans for trust (social engineering). With the help of this technique a duped user himself/herself grants permission to the deactivation of his/her own protective applications, because he/she thinks that the web page or the program being encountered is totally legal and interesting and important to him/her. Only continuous and up-to-date warnings, information and the regular training of users can provide protection against such techniques that exploit human gullibility. Looking at the arch of development it can be seen, that in the future we must expect ever more technically refined attacks that will be increasingly difficult to prevent or to avoid.

The threat of internal treachery

Cyber-Ark has conducted a survey of 300 senior IT professionals of companies that each employ over 1,000 people.

- Half of those asked have admitted that their administrator passwords granted them access to information that they did not need for their work;
- Almost a hundred have admitted that they also had access to confidential information, such as the details of wage payments, personal email messages and minutes of meetings;

- A third of all administrative passwords are changed only once a quarter, while 9% remain constant, granting access to the employee even after he/she has long departed from the firm;
- Half of those asked have said that they need not ask for permission or authorisation from anyone to query any confidential information.

In addition to factors that threaten systems in live operation there are security risks also in the development process. The most evident example for this would be a malicious developer inserting code into a banking system to result in functions reflecting neither the intentions of the bank nor the intentions of the customer, such as to forward the user's password to an external e-mail address.

Information disclosure obligations of financial organisations in relation to their services provided over the internet

Pursuant to the related statutory provisions financial organisations providing online services have information disclosure obligations as follows:

- 1 The fees and the costs of online services must be made accessible to customers electronically as well;
- 2 Customers must be provided clear and complete information about the risks of online services (provided over the internet) and about the related minimum hardware and software requirements prior to signing a contract for the service. Customers must be provided accurate and articulate information about their special rights and obligations related to the online services and about the rights and undertaken obligations of the financial organisation, including situations caused by problems due to system errors and internet security vulnerabilities.
- 3 Adequate information to customers is of emphasised importance if there are novelties appearing in the internet-based services of the financial organisation, especially if these are related to identification or some other internet security function.
- 4 Financial organisations must accept and acknowledge that the use of legal or technical language could cause understanding difficulties for customers; the information is therefore to be made available using everyday language that is intelligible for everyone.
- 5 The contractual terms and conditions for online services must be easily accessible also within the service, just like the rules of the security and confidentiality regulations pertaining to customers.
- 6 Customers must be informed about the system for the management of complaints and reporting related to online services, about the procedures to be followed in case of service problems, about the means of legal remedy and about the formats and deadlines for responses undertaken by the institution.
- 7 If cyber criminals have obtained unauthorised access to a customer account, the financial organisation is obliged to inform the customer as soon as possible in detail about what has happened, about the consequences to be expected, about the things to do and about the liabilities for damages.

The professional literature used in this Recommendation

- ISO 27001 – 27005
- ISACA: „GENERAL CONSIDERATIONS ON THE USE OF INTERNET”
- ISACA: „IS AUDITING GUIDELINE INTERNET BANKING”
- European Payment Council: „Customer-to-bank security threat assessment”
- ENISA (European Network and Information Security Agency) „Methods for the identification of Emerging and Future Risks”
- PTK – CERT-Hungary (2007): „Internet threats affecting financial institutions”
- MTA-SZTAKI: „Security risks and controls in the information technology network infrastructure”
- FFIEC (Federal Financial Institutions Examination Council): „E-Banking”
- FFIEC (Federal Financial Institutions Examination Council): „Authentication in an Internet Banking Environment”
- COMMISSION OF THE EUROPEAN COMMUNITIES: „Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan”
- Basel Committee on Banking Supervision 2003: “Risk Management Principles for Electronic Banking”
- FATF 2008: “MONEY LAUNDERING & TERRORIST FINANCING VULNERABILITIES OF COMMERCIAL WEBSITES AND INTERNET PAYMENT SYSTEMS”
- ENISA (European Network and Information Security Agency) „Security Economics and The Internal Market”
- Michel J.G. van Eeten and Johannes M. Bauer: „ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES”
- CRAMM: CCTA Risk Analysis and Management Method
- Finjan: Web Security Survey 2008
- Cisco: Internet Malware Trends 2008