Theoretical and Applied Economics
Volume XIX (2012), No. 4(569), pp. 59-78

Non Security – Premise of Cybercrime

Ion IVAN
Bucharest Academy of Economic Studies
ionivan@ase.ro
Daniel MILODIN
Bucharest Academy of Economic Studies
daniel.milodin@ase.ro
Cătălin SBORA
Bucharest Academy of Economic Studies
catalin.sbora@gmail.com

Abstract. *It is presented the concept of cyber crime. There are detailed the vulnerabilities of IT applications. There are listed the types of Internet fraud. There are analyzed the predisposing factors of cyber crime. There are identified the deficiencies of the security systems. It is build a model for information security management.*

Keywords: cyber crime; applications; vulnerabilities; skimming; phishing.

JEL Code: C63.
REL Code: 9J.

1. On-line applications and cyber crime

The informatics application defines computer software designed to automate and increase efficiency of human activities in both the virtual and real environment. The applicability domain of the software products starts from simple processes such as forms' loading and printing and continues with complex processes that are part of software technology such as the electronic product manufacturing stages.

The main role of a computer application is to take over and facilitate the work of the human factor. Also, using computer applications it is assured users access to products and services.

In the online services, computer applications take the user interaction component, assuring him the possibility of documentation of products, of choosing the desired products, and the possibility to pay the products, but within the on-line control operation should be interposed human factor, its role being to provide transport between online store and customer. Computer applications are based on a set of software and hardware components, the hardware components are providing the equipment necessary for the application functionality and the software components assure the application's programs. A computer system consists of: computers, data transmission systems, other hardware components, software, processed data, personnel operating the computer, theories underlying processing algorithms (Ivan, Ciurea, 2009).

Internet, as a large computer network, is developing each year in explosive rate, becoming the base of all informatics' technology. The Internet is an information "network of networks" gathering thousands of unrelated networks coming from dozens of countries. It is a virtual network consisting of a growing number of LANs (Local Area Network-LAN) – public and private wide area network (Wide Area Network – WAN), regional and national networks interconnected (Ivan, Apostol, 2003, pp. 32-38).

Amount of information stored and accessible on the Internet is growing rapidly. Research on the Internet topology shows that in the apparent chaos of the Internet there are independent scale and self-organization characteristic. Thus, Barabasi et al. (2000) show that *www* diameter, defined as the shortest average distance between two sites, was in 2000 more than 19 links. Because of logarithmic dependence Internet volume, even a 1000% increase in the number of links *www* will not rise above 21.

Internet, as a network, continues to provide development support. Technologies and applications provided through the *World Wide Web* evolve into an alert rhythm, providing both variety and utility. Currently, most services from the real world find their virtual equivalent, accessible via the Internet, the main advantage of the Internet is time saving, because the process of accessing services is automatically and it is not necessary to be present in a given geographical area in order to access Internet services.

But the Internet has some shortcomings that are generated not necessarily the technology itself, but rather by the human factor. The shortcomings are related to the confidentiality of information that is circulated through the Internet. Because of the complexity and heterogeneity of systems that are interconnected via the Internet, it is difficult to ensure full confidentiality of information, considering that it is sufficient that at some point in one of the systems considered safe to be discovered a vulnerability allowing unauthorized access to that system resource.

The first incident based on the exploitation of vulnerabilities in operating systems was recorded in 1988 with the advent of an application that was created for scientific purposes, for determining the size of the Internet; this application is called Morris Worm[(1)]. The reason why the application was considered dangerous is the fact that the spread in the network and run automatically without user permission, exploiting certain vulnerabilities of operating systems, existing the possibly that someone would use this application to collect information personal. There was an increase of incidents of this kind and then a variety of other types. Along with a increasing amount of data presented on the Internet grew, the cyber attacks have taken a larger area.

Electronic theft has become a permanent presence for storage, processing and transmission data in the online environment. Today, the concept of cyber crime is a form of criminal activity which consists in obtaining confidential data, and data access for applications like banking, e-commerce applications or information on credit cards, using data manipulation techniques identity of a person or an institution.

Electronic deception the most common and best known method of cheating by electronic means is *phishing* operation, a procedure whereby a user of electronic financial services is misled to communicate confidential information to unauthorized persons. This information is used later to gain access to the victim's bank accounts to withdraw money from these accounts or to pay for various services and products. Techniques and methods used by criminals are the most diverse. For example, bank customers are contacted by phone for a specific bank and are asked the identification codes for access to their accounts, justifying the need to update the data bank's computer system.

Another way often used through the Internet is sending official-looking e-mails which advise users to access certain websites with which are then collected personal data of users. These websites are copied, the technical term is cloned site, at the graphic level, usually after the official websites of financial institutions, easily fooling the average user. Phishing operation gained momentum with widespread of the online banking services due to the possibilities arising from the opening of the Internet, and the lack of an organization to regulate and control access to financial transactions. Another factor contributing to the success of phishing attacks is naive users combined with the lack of adequate training on how to use and protect personal information.

As illustrated in Figure 1, based on statistics provided by RSA[2], the number of phishing attacks is increasing as there are new tools that facilitate the creation and development of phishing attacks. These tools provide offenders who have very strong knowledge of computers access to advanced technology, and therefore it is normal to the number of attacks since the number of individuals who launch these attacks increases.

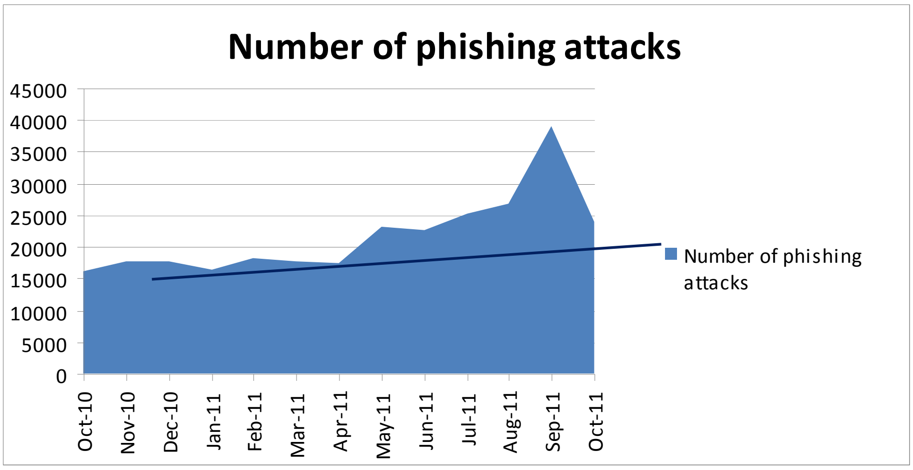

Figure 1. *The evolution of phishing attacks in 2011*[2]

These sets of tools called phishing kits evolves and becomes an industry. If some time ago who thought and implement mechanisms phishing was the one who actually launch attacks, currently phishing solutions are implemented by well organized groups that sold on these sets of tools to those who are willing to use them and ready to pay for them.

A set of specialized tools for phishing attacks include:

- one or more specialized computer programs used to create a database with e-mail addresses which are used to reach targets attack;

- one or more software or plug-in for web browsers that can be used in a Man-In-The Middle architecture to check in real-time the validity of information provided by the user;
- scripts that are used to determine system specifications used by the victim, these specifications is limited in most cases at: screen resolution, Internet browser version, the time zone in which the user is located, etc.;
- automated tools that scan sites used as the target of the attack, for automatic extraction of graphic symbols, HTML sources and other elements used to help generate further authentication pages that are graphically identical with the original page.

As shown, the trend is the developing of multi-level criminal structures, which makes it more difficult to identify and remove items that are based on this type of crime. However, with automation and use of templates attacks becomes possible to create security solutions to identify phishing attacks before they affect end users. Most security solutions providers have added in the existing modules additional mechanisms to detect unauthorized access (Intrusion Detection System) to monitor content that is displayed by Web browsers, as well as modules for filtering electronic messages (Spam Filters) to reduce risk user to receive electronic messages from servers that are considered high risk. Going forward, creating a viable architecture for rapid detection and stop this type of attack requires the use of collaborative mechanisms between security solutions, so that when a security solution detects a phishing attack template, that template to be distributed in real time to other security solutions. Currently this is done easiest using solutions from the same manufacturer, the main reason why is more difficult to implement an architecture that allows inter-operation solutions from several manufacturers derives from the fact that there is no protocol or a way to inter-operate between different solutions for security vendors, and also because is involved the human factor, through the need to form a working group bringing together several companies producing security solutions for establish a standard for storing information about phishing attacks.

Architecture options for intercommunication between two or more security solutions are the option to connect peer-to-peer interconnection option through servers' zonal coverage. The two architectures are shown in Figure 2 and Figure 3.

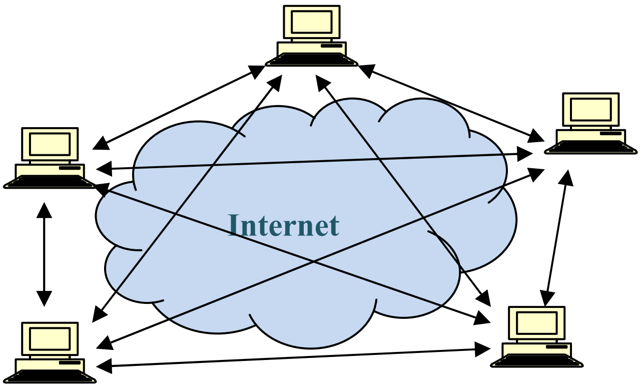

Figure 2. *The peer to peer configuration*

Note that for peer-to-peer architecture, in order to avoid loops by propagating the same template multiple detection methods, it is necessary to identify the protocol level, to determine when there is a need for a particular template.

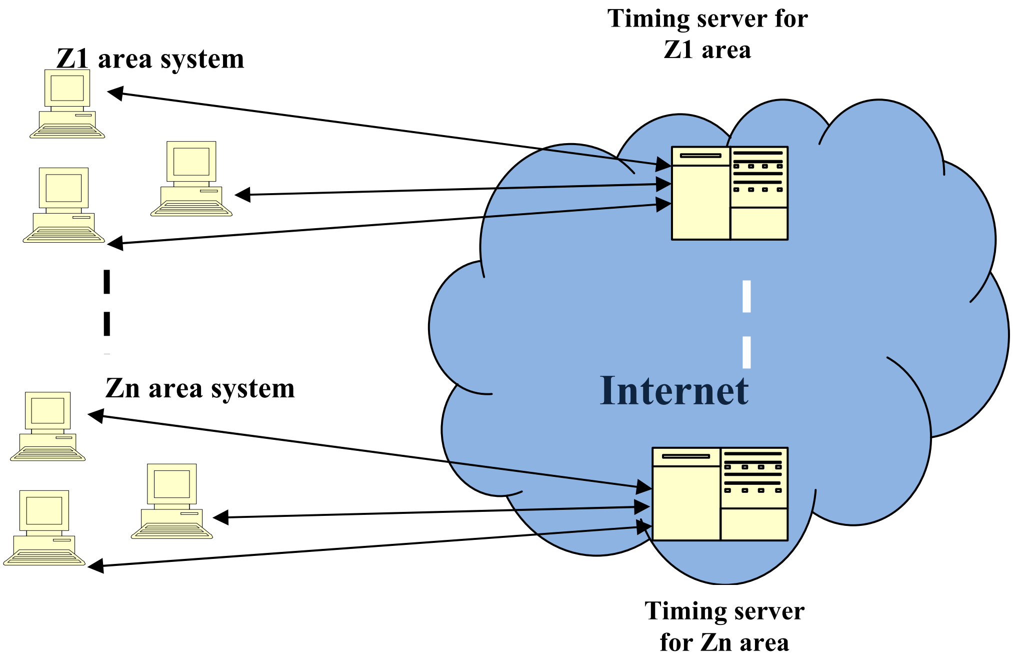

Figure 3. *Configuration with synchronization patterns through regional servers*

Solution with servers' regional advantage is the fact that more easily adapts to current security solutions compared to solutions using peer-to-peer model, primarily because it does not generate a dependency between existing security solutions, but based on a fixed structure of the information on the synchronization server. In this way each manufacturer is free to implement and optimize solution as end-user wants.

Another aspect that is treated differently to optimize resources and effective solutions in a server-based architecture area is related to the fact that cyber attacks vary in intensity and complexity from area to area as illustrated in Figure 4, where is the distribution of phishing attacks globally, the graph is made on the same data set as that used in the graph in Figure 1. Another thing shown in Figure 4 is that most attacks are directed towards the citizens of countries with developed economies and the banking systems are quite advanced and have reached a degree of maturity.

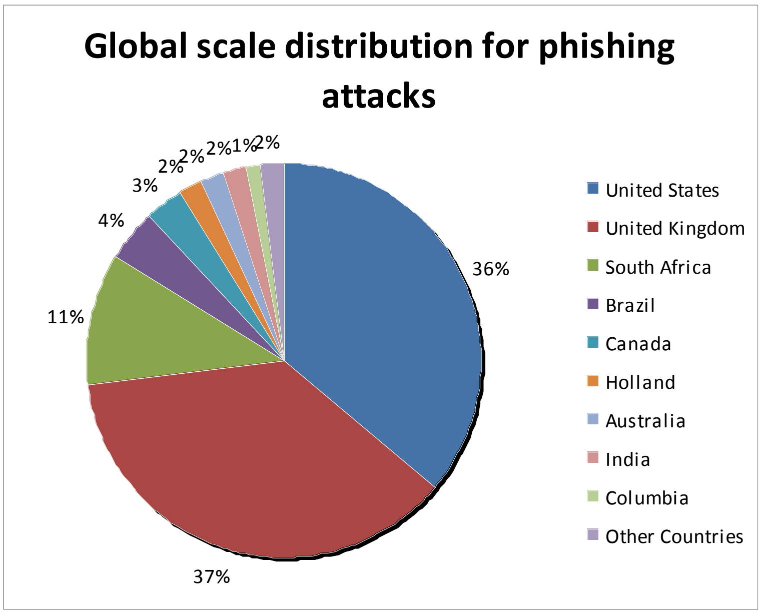

Figure 4. *The globally distribution of phishing attacks*(2)

Form all the methods of fraud over the Internet, phishing is one which requires that the attacker to be quite solid knowledge in computers and writing software in languages that allow access to any area of memory. Much of the fraud conducted over the Internet is based more on ingenuity and creativity in terms of deception than on their outstanding technical skills. These frauds which depend on technical elements only to a lesser extent are quite difficult to control, using technical means (security solutions), and success or failure of these scams depend mostly on the human factor and its ability to identify fraud attempts. Are presented ways to defraud involving the technical elements used by a regular user of Internet.

Fraud by charging, by which the person concerned is required to pay in advance a series of taxes, will receive in exchange a certain amount of money or prize items. These fees are usually as processing fees, postage or fees for carrying out notarial acts. The victim pays these fees and receives nothing. The best example for this type of fraud are *Nigerian letters*, which the victim is important promise percent in exchange for helping to transfer large sums of money from a foreign country. In another scheme of fraud, the victim is convinced that won a major lottery, but that does not exist.

Fraud involving online auctions are conducted either by presenting auction sites a false object, which the offender belongs or does not meet the conditions set out in the notice, or by the fact that, after collecting money, the offender did not send product the transaction.

Fraud involving investments in which the offender submit a quote containing investment proposals requests for loans have certain services that are obtained as a result of an investment. Victims who send money as a result of receiving these e-mails will never get the promised services or goods of the offender.

Business fraud or Employment fraud type involves stolen identity, a scheme to refer to goods and counterfeit checks. The initiating fraud places a job on one of the sites with job offers from Internet. Those who respond are requested confidential personal information such as date of birth and social insurance number. They will then be used by the initiator fraud to buy goods on credit. They are sent to another person who answered the ad and was hired by the offender to receive merchandise. This return product to the originator fraud. Offender, which usually appears as a foreign company, pays the person who sent back check fake products that usually contain a higher amount than that required for shipping charges. The difference in money is transferred back to the person making the delivery of the offender, before the fraud is discovered.

2. Vulnerabilities in computer applications

The vulnerability of computer applications is given by the fact that information is lost, stolen, modified, improperly and illegally decrypted first source of vulnerability is given by the equipment used, the implemented software and database system used. Vulnerability is strictly related to equipment reliability, equipment ensuring reliable and continuous operation parameters systems hosted on the improper equipment contributing to the improper operation.

Software vulnerability is given mainly by computer viruses, while vulnerability database is directly connected with unauthorized access to stored data and the destruction intentionally or by accident of the data.

The most common vulnerabilities of computer applications are given in Figure 5:

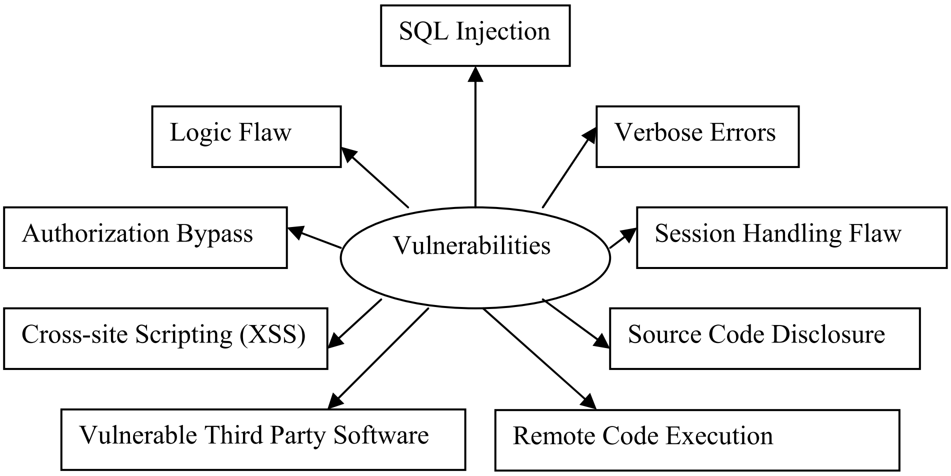

Figure 5. *Types of applications' vulnerabilities*

- *SQL Injection* is based on the fact that most web projects use databases to store and sort data. Structured Query Language (SQL) is used to access information from a database, its syntax differs slightly for different database servers, but SQL is a universal language suitable for all databases.

A vulnerability called SQL injection, SQL injection in short, occurs when an attacker enter any data in a SQL query or when, by injecting syntax, logic statement is modified in such a way as to perform a different action. The best way to defend against SQL injection routines are based on strong input validation.

Logic Flaw assumes that even for the simplest web application development requires a large amount of logic for each stage. This logic provides an opportunity for logical errors and logic errors provides a very basic range of attack, but are overlooked because they are scanned with specialized programs in identifying vulnerabilities.

Logical errors occur when the programmer or web developer doesn't consider all the effects it has on the application code written by him.

Authorization Bypass is based on the process of determining whether a user using a certain identity has permission to access a resource or not, and after checking granting him access to that resource is in accordance with system policies, regardless of the identity his real called authorization.

Vulnerabilities related to authorization and access appear anywhere in the web application, and refers to what happens when an attacker has access to a resource that would normally have access only authenticated users or who have certain privileges in those applications

- *Cross-site Scripting (XSS)* XSS is an attack technique, used to force a webpage to display a malicious code (written usually in HTML (Hypertext Markup Language)/JavaScript (also called malware)), which is then executed in a user's browser. This type of attack does not target server Web site (this is just a host), but malicious code is executed directly in the browser, because the real target of the attack is the user.

To infect a browser, must be visited a page that contains malicious JavaScript!

- *Vulnerable Third Party Software* assumes that applications taken from other companies or other users are considered safe by default. Many web applications from third parties are uncertain. For protection in these cases is advisable to check and test applications taken from third parties.
- *Session Handling Flaw* includes aspects of data handling user authentication and session management of its assets. Authentication is a critical process of this aspect, but even the strongest authentication process is undermined by the errors of management functions to verify credentials, including: changing passwords, forgotten password recovery function, the function of remembering passwords by application web updates accounts and other related functions. To avoid such problems, for any functions related to account management, user must then log in, even if it has a valid session id.

Internet user authentication requires at least a username and password. There are safer ways to market type authentication hardware and software based encryption and biometric tokens, but they are not very popular due to high costs of purchase. A wide range of errors related to accounts and session management resulting from the compromise of user accounts or system administration.

Verbose Errors they are not really a type of attack, but error messages are usually containing complete paths and file names, descriptions for the database schema, errors connected to the applications back logic and the environment where they are running.

A typical form used for authentication requires for the user to complete two fields (user name and a password), other applications, though, are asking for more information (birthday, PIN code). When an authentication process fails, there are applications that are detailing the cause of failure which can generate security issues and can ease the success of a brute force attack.

- *Source Code Disclosure* is a frequently encountered coding error, which more obvious in script based languages that are meant for web applications. This can be exploited by an attacker to obtain the source code for the application and configuration files through HTTP. Many of the web pages make available for the user files to be downloaded by using dynamic web pages. When the web browser asks for a page, that page will be executed on the server returning the result the web browser, so dynamic web pages are pieces of code that are being executed/interpreted on the server before returning any result to the user's browser. If the web application is not secure enough it is possible for an attacker to be able to download pieces of the source code, allowing him to create an image about the logic behind the application and identify the way that the web application is handling the requests, the parameters for these requests, database schema, potential vulnerabilities in the code, so having the source code makes it easier for an attacker to prepare his attacks on a given application.
- *Remote Code Execution* this kind of vulnerabilities allows the execution of an arbitrary set of instructions, in the security context of a legitimate application. Considering that these instructions set is being controlled by an attacker, these vulnerabilities are becoming very dangerous, especially in the cases where the vulnerable applications have access to the operations that are being executed at the operating system level.

Vulnerabilities diminution when speaking about informatics applications is being done by imposing measures of access control and the increase of applications' reliability. All these are being done by having a cost attached and this cost is becoming less significant when the measures are being taken during the design and implementation phases for the system.

It is considered:

S – the users set, composed by elements $s_1, s_2, ..., s_i, ..., s_{NU}$;

NU – number of users;

A – the set of records in the database, containing elements $a_1, a_2, ..., a_i, ..., a_{NA}$;

NA – number of records in the database, that are part of set A;

H – set of executable instructions for the software product, containing elements: $h_1, h_2, ..., h_i, ..., h_{NH}$;

NH – the number of executable instructions for the software product;

F(X,Y) – analytical function for computing the difference between X and Y sets, with [0; 1] codomain; if F(X,Y) = 0 then the two sets have no common element; the more F(X,Y) becomes closer to 1, the more the two sets are alike; the more F(X,Y) becomes closer to 0 the more the two sets are different;

$G(s_i)$ – function defined on S taking values in S, corresponding to behavioral changes for the users;

$D(a_i)$ – function defined on A, taking values in A, that corresponds to the changes in the content of the database records;

$C(h_i)$ – function defined on H, taking values in H, which corresponds to the changes in the source code of the application.

Usually, functions G(), D(), C() have a definition based on resources that are being used for doing changes, some of them controlled by the application's administrator, some others controlled by those that introducing non-secure elements. For each of these functions a graph will be assigned.

Identifying vulnerabilities means finding, on the graph associated to each application, those edges that are producing changes over the sets S, A, respectively H, changes that are being appreciated both by the administrators and the users, like having undesired effects over the objective for which the application was built for.

Considering a set $T=\{t_1, t_2, ..., t_i, t_{i+1}, ..., t_{NT}\}$, where NT is the number of time moments and it will assigned to the sets S, A and H, time moments, so that $S(t_i)$ represents the set of users at the moment t_i, $A(t_i)$ represents the set of records in the database at the time moment t_i and $H(t_i)$ represents the set of instructions that are included in the application at the moment t_i.

Function F(X,Y) establishes, in this context, if there are differences between the same sets at different time moments, which imposes the next relations to be calculated:

$F(S(t_i),S(t_{i+1})) = k_1$;

$F(A(t_i),A(t_{i+1})) = k_2$;

$F(H(t_i),H(t_{i+1})) = k_3$.

Depending on the values that were calculated for k_1, k_2, k_3 and depending on the graphs' edges that led to these values it will be concluded if the transformations are the result of some transaction made through the application or they are the effect of the non-security.

3. Ways to reduce insecurity

Reducing the insecurity is being resumed, most of the times, to covering vulnerabilities either by updating vulnerable applications, either by using some third party specialized applications that are offering protection against zero-day attacks. The zero-day attacks that are often encountered are those that are using SQL Injection techniques and that most of the time are exploiting vulnerabilities that are coming from the development and quality assurance processes, so the first measure that can be taken in order to reduce this kind of vulnerabilities involves directly the awareness of the people involved in the development process so that they can see the necessity of avoiding situations where the user is allowed to indirectly create dangerous SQL queries, by using the information that is introduced in the forms without have strong validations enforced.

In the development stage the following techniques are being used for eliminating or reducing the risks related to SQL code injection:

- use of prepared statements;
- use of stored procedures;
- validation for the inputs received from the user, before effectively using these to build SQL queries;
- use of ORM frameworks (Hibernate, Entity Framework, etc.).

These techniques can come with additional time at the beginning of the development, due to the need of extra analysis and the need of having a structured code from the beginning, but long term, the use of these kind of techniques reduces the costs of development, maintenance and update for software applications.

The use of security applications capable of preventing SQL injection attacks introduces, most of the times, additional processing, and this fact will affect the performance of the application in the cases where an intensive usage is needed.

Another class of vulnerabilities with a serious impact, in a compromised system, is represented by remote code execution. This type of vulnerability appears most of the times due to the way the code in different informatics applications, “buffer overflows” problems being those that are allowing arbitrary code execution that will initiate remote attacks.

The code that initiates the attack is usually a TCP/IP client that connects to a remote server, from where it will receive different commands that will be executed on the host system, so the attacker will get to have unlimited access to the resources from the compromised system.

The attacks that are using buffer overflow techniques rely on binary code execution from the data segment. This has permitted for some new hardware technologies to be developed in order to prevent the execution of code from the part of memory assigned for data usage *DEP – Data Execution Prevention* and they are implemented at the micro-processor level, by using methods for marking executable memory areas, and any attempt to execute code from outside that area will be blocked.

Another technique used for execution of remote code is based on exploiting web servers configuration vulnerabilities, so that Denial of Service problems are being generated, the information associated with the users of the web applications is being compromised together with the entire functionality inside the web applications that are hosted on the vulnerable web servers.

Taking into consideration that the possibility of executing remote code has a main action vector, the existence of a network link, no matter if that is an internal network or Internet, the options that we have for protecting against this kind of threats is to use specialized software applications that are able to monitor the traffic, firewall and Intrusion Detection Systems.

Vulnerabilities found in the operating systems have the largest target pool, first of all due to the fact that each modern device that is capable to run a informatics system has an underlying operating system. The important providers for operating systems are releasing security updates at least once a month, for covering the problems that are being discovered in the different usage scenarios, after constantly watching and analyzing the way that the systems are being used. Microsoft, for example, the company that develops the Windows operating systems, provides security updates for the users in the second Tuesday of a month and this day was named by the IT specialists the Patch Tuesday.

Together with update patches, the company also provides Information Bulletins where the technical details and the reasons for which those updates are needed. These updates are being distributed to the OS users automatically or by manual update, being recommended to have the system configured to run automatic updates with an update interval set for at least once a day.

So, for increasing the security and reducing the possible vulnerabilities it is very important for the operating system to have the latest updates. In a large organization with a high number of informatics systems it must be implemented a strategy and the things need to be organized for taking this updates. This is necessary, first of all, to avoid the overload of the external network connection and the overload for the update servers, as these things will just generate problems, by the simple fact that the systems will be unable to get the updates in time and they will be exposed for unlimited time against the possible threats that are covered by the update patches.

The most efficient way to avoid the overload for the external connection is to use one or more internal servers for the update process, the purpose for these servers is to take the updates from the original update servers and to ensure that they are safely distributed in the internal network of the organization. In Figure 6 we have the structure that we discussed.

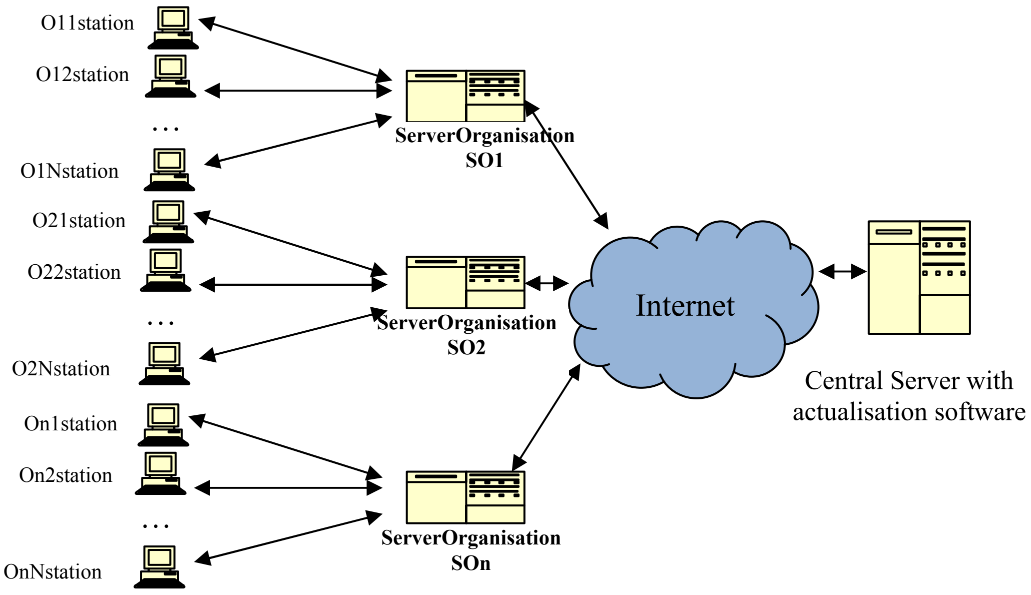

Figure 6. *Tree structure for offloading the update servers*

Using an internal server increases the efficiency of the way the internal and external resources are being used, by reducing the traffic on the external connection and the time needed for getting the updates.

4. Predisposing factors of cyber crime

Cyber crime is justified, most of the times, by huge financial earnings with relative low effort in a short period of time. This type of criminality is based on different vulnerabilities, discovered within the software applications that were created to facilitate and improve activities specific to the humans, but it is equally generated by the naivety of the people that are using these applications. Software applications are usually very complex, both from the point of the logic that is implemented and from the point of the functionality, and this fact leads to situations where not all of the variables that affect the functionality are taken into consideration and in this way the vulnerabilities and the security problems related to data handling arise.

So, one of the factors that contributes on creating security breaches and favoring the cyber crime is actually the complexity of the software applications and the large number of functionalities that is being implemented inside these applications, the more complex an application is, the more chances to find security breaches.

Most of the times the users are those that are making the life of cyber criminals easier, showing more than naivety when they are engaging in financial transactions with persons or companies that they don't know and for which they don't have any guarantee. From the factors of cyber crime that are mostly dependent on the human factor we enumerate:

- Usage of on-line payment methods in unsecured working environments;
- Providing personal information on dubious websites;
- Not using specialized sites for certain activities, sites that have a high degree of certification;
- Paying in advance, without having the confirmation that the products were actually sent;
- Providing additional personal information, when this information is not really needed to validate the transaction.

Paying more attention to the information that is requested when completing a transaction, reading all the conditions involved, verification of the websites that are used for e-commerce will contribute on reducing the number of people that being cheated in the electronic environment.

The main cause for online cybercrime is related to the human factor. Regarding this aspect, it is necessary to increase the level of awareness regarding the danger that comes from the electronic theft. One that know this kind of frauds will be more careful when navigating the Web. The education of the user in order to prevent these methods of committing frauds is one of the first steps for effects diminution. Have a better knowledge for the danger that he is exposed, the user will be able to analyze that he has when accessing a website. It is well known the fact that many were cheated through false promotions where they were asked to transmit a given message in order to gain some benefits, in fact those messages were recharging the cards for mobile phones, owned by the crooks. Understanding and being aware of the danger to be robed by electronic means the user will avoid providing identification information to unknown people.

Technically speaking the factors that are contributing on creating security breaches are generated by the fact that, during the development process for the software applications, the attention paid to security aspect is very low, the attention being directed more on the correctness of the implementation from the logical point of view, compared to the functionality requirements.

Releasing the software products on the market without packing the binary code, that is the result of the source code is another factor that has an important contribution in reducing the effort that cyber criminals are putting for compromising a software application. Packing the binary code involves encoding the executable code in such way that when someone will try to disassemble/decompile the executable code it will not be able to easily understand the logic behind and more important it will not be able to identify possible vulnerabilities in the code.

Additional to packing the executable binaries, it is also recommended to sign the applications with digital certificates, allowing the users to identify the situations where different components of the application were replaced (after a virus infection for example), allowing to a potential attacker to execute his commands in the context of a legitimate user/administrator, increasing the abilities that the virus has for spreading on even more systems and do more damage. So having applications that are not digitally signed is another risk factor.

Knowing the factors that promote insecurity allows the development of techniques and methods to cope with and prevent attacks.

5. Deficiencies for the security systems

Security systems that are used for protecting information systems are also informatics applications, being exposed to security threats in the same way as regular applications, the difference being that most of the security applications have their own mechanisms implemented for protecting against tampering attempts, considering actions as trying to force the termination of the processes included in the solution, code injection, etc.

Most of the times, security systems are complex systems, that require advanced technical knowledge for implementation; this a reason for which it is possible to have security flaws inside security systems, and examples can be found even for the most important players on the security solutions market. Security systems are usually specialized on certain types of attacks and vulnerabilities and most of the times they will not offer 100% protection against cyber-attacks, thereby most of the times it is necessary to use many security solutions for protecting a system and getting a higher degree of security. The systems that are widely used are those for detecting and preventing malware infections, with a mechanism that implies detecting the infections based on some signatures included in a local database that should be synchronized daily with a central database being updated by the security laboratories.

The number of malware applications created each day, reached 73000 in march 2011, according Panda Security[(3)], which makes this protection mechanism to lose its efficiency, due to the large volume of information that needs to be updated and distributed to the users and if consider the fact that at some point there will be users that have wrong configurations, and they will not be updated in time, we have already some obvious issues with this approach.

Even if we assume that at some point the synchronization is up to date, it is highly unlikely that these updates will cover all of the new malware applications, so this approach will always lead to situations where the cyber criminals are one step ahead. For this reason, some of the antivirus providers have started to provide solutions that are based on detecting the behavior of the applications in order to identify malware actions. This technology is called *Behavior-Based Malware Detection* and is most of the times implemented by using heuristics methods.

This technology is still under-developed and it is usually used together with the conventional methods, based on signatures. One of the problems that is often encountered in the behavioral implementations is related to the false alarms (False Positives) because there is always possible that a normal application to reproduce partially or totally the behavior of a malware application.

The efficiency of anti-malware systems, E, will be determined based on at least two factors:

- Correct detections percentage
- Undetected threats percentage

using the following formula

$$E = \begin{cases} [PAC + (100 - PAN)] / 2, PAN <> 100 \\ 0, PAN=0 \end{cases}$$

PAC – correct alerts percentage, from the total number of alerts;
PAN – undetected threats percent.

Starting from this way of measuring the efficiency of a security system it can be established if the system fits the needs or not.

Security systems deficiencies are dependent by the nature of the informatics systems where the security components are integrated. In the case of banking systems, most of security deficiencies are showing up due to the naïve user's behavior, due to the wrong way of handling personal and confidential information and especially from implementing incomplete security procedures that will not respond in real time to external challenges received by the informatics systems.

Having a vision to prevent security issues and to implement safety procedures that will run in new situations will reduce security breaches.

In the informatics systems it must be taken in consideration the implementation for a procedures regarding the response time, which will help identifying the true owner of the accessed data.

Going over the boundaries of the preset times enables the execution of some safety applications that will even inform a human operator that will validate the problem. Implementing the procedures based on the response times, will ensure a minimum time for manipulating the data used for accessing the system, the delays being specific to situations were unauthorized persons try to access the systems. Also, mixing procedures based on access times with procedures based on having unique access keys will lead to a superior securing for informatics systems.

Also, linking procedures based on access times using procedures based on unique introduction of access keys lead to superior security of the informatics' systems.

6. Conclusions

According to a recent study of the Symantec company[(4)], from the financial point of view, the annual loses, seen at a global level, that were caused by cyber crime were evaluated to 114 billion dollars, on this we need to add also the indirect loses that were generated as a consequence of the security incidents recovery. So as we can see the non-security generates a series of problems that eventually, in the case of companies, will be directly reflected in financial loses.

There is no perfect security system that will ensure in the same time total protection for all classes of users, but using the right security systems, dramatically reduces the possibility for the information to be compromised. It is very important that each user to be aware of the risks that he is exposed to and to choose the security system that offers protection according to his needs. It is needed that the scientific research to generate new techniques, methods and instruments that will prevent the effects of insecurity, and also to foresee the new challenges and to be one step ahead by prevention. As it can be seen the cyber crime got through many evolution stages, starting from a simple attack on a computer, using a computer virus, reaching to attacks over an entire economical branch. The danger of cyber crime is growing as it involves stealing information that is considered to be private and allows accessing to personal resources of the people. In order to increase the protection over these attacks, caution must be taken from the first steps when creating informatics systems, reducing or eliminating the risk of propagation over the users that are using computing resources.

Notes

[1] Carnegie Melon Software Engineering Institute, Security of the Internet, Froehlich/Kent Encyclopedia of Telecommunications, vol. 15.

[2] See RSA Fraud Report, Noiembrie 2011, http://www.rsa.com/

[3] http://press.pandasecurity.com/usa/news/creation-of-new-malware-increases-by-26-percent-reaching-more-than-73000-samples-every-day-according-to-pandalabs/

[4] See http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02, accesat Ianuarie 2012.

References

Barabasi A.L. et al., „Scale free characteristics of random networks: the topology of the world-wide web, Physica A, *Elsevier Science B.V.*, 2000

Goloşoiu-Georgescu Ligia (2003). *Mijloace, modalităţi şi instrumente de plată*, Editura ASE, Bucureşti

Ivan, I., Apostol, C., „Certificarea produselor program prin amprente", *Revista Română de Informatică şi Automatică*, vol. 13, nr. 1, 2003, pp. 32-38, ISSN 1220-1758

Ivan, I., Ciurea, C., „Quality Characteristics of Collaborative Systems", *Proceedings of The Second International Conferences on Advances in Computer-Human Interactions*, ACHI 2009, February 1-7, 2009, Cancun, Mexico, paper published by IEEE Computer Society Press and IEEE XPlore Digital Library, ISBN 978-1-4244-3351-3

Ivan, I., Toma, C., „Testarea interfeţelor om-calculator", *Revista Română de Informatică şi Automatică*, vol. 13, nr. 2, 2003, pp. 22-29, ISSN 1220-1758

www.bnro.ro