Optimizing Anti-Phishing Solutions Based on User Awareness, Education and the Use of the Latest Web Security Solutions

Ion LUNGU[1], Alexandru TĂBUŞCĂ[2]
[1]Academy of Economic Studies, Bucharest, Romania
[2]Romanian-American University, Bucharest, Romania,
ion.lungu@ie.ase.ro, alextabusca@rau.ro

Phishing has grown significantly in volume over the time, becoming the most usual web threat today. The present economic crisis is an added argument for the great increase in number of attempts to cheat internet users, both businesses and private ones. The present research is aimed at helping the IT environment get a more precise view over the phishing attacks in Romania; in order to achieve this goal we have designed an application able to retrieve and interpret phishing related data from five other trusted web sources and compile them into a meaningful and more targeted report. As a conclusion, besides making available regular reports, we underline the need for a higher degree of awareness related to this issue.

Keywords: *Security, Phishing, Ev-SSL, Security Solutions*

1 Introduction

Phishing is the term for the operation of cheating network users to provide private information for identity or business theft. This issue is one of the most important threats today for both consumers and businesses depending on the IT infrastructure. During the last five years phishing has been growing rapidly, with an estimate citation of approximately 8 million daily phishing attempts all over the world [4].

The international organization of APWG - Anti-Phishing Working Group – has reported that during the second half of 2008 the number of phishing attacks reported to them grew with more than 20 percent related to the figures of the first half of the year, from 47342 to 56969 [1].

2 Web Threats in the Today IT Environment

Attacks on vulnerabilities in web applications began appearing almost from the beginning of the World Wide Web, in the mid-1990s. Attacks are usually based on fault injection, which exploits vulnerabilities in a web application's syntax and semantics. Using a standard browser and basic knowledge of HTTP and HTML, an attacker attempts a particular exploit by automatically varying a Uniform Resource Indicator (URI) link, which in turn could trigger an exploit such as SQL injection or cross-site scripting.

```
http://rau/test.cgi?a=1
http://rau/test.cgi?a=1'
-> SQL Injection
http://rau/test.cgi?a=<script>…
-> Cross-site Scripting (XSS)
```

Some attacks attempt to alter logical workflow. Attackers also execute these by automatically varying a URI.

```
http://rau/test.cgi?admin=false
http://rau/test.cgi?admin=true
-> Increase privileges
```

A significant number of attacks exploit vulnerabilities in syntax and semantics. You can discover many of these vulnerabilities with an automated scanning tool. Logical vulnerabilities are very difficult to test with a scanning tool; these require manual inspection of web application source code analysis and security testing.

Web application security vulnerabilities usually stem from programming errors with a web application programming language (e.g. Java, .NET, PHP, Python, Perl, and Ruby), a code library, design pattern, or architecture.

These vulnerabilities can be complex and may occur under many circumstances. Using a web application firewall might control effects of some exploits but will not resolve the underlying vulnerabilities.

Web applications may have any of two dozen types of vulnerabilities. Security consultants who do penetration testing may focus on finding top vulnerabilities, such as those in a list published by the Open Web Application Security Project (www.owasp.org). Other efforts to systematically organize web application vulnerabilities include six categories published by the Web Application Security Consortium (www.webappsec.org). The following descriptions of web vulnerabilities are modeled on the Web Application Security Consortium proposed schema.

Authentication – stealing user account identities

- Brute Force attack automates a process of trial and error to guess a person's username, password, credit-card number or cryptographic key
- Insufficient Authentication permits an attacker to access sensitive content or functionality without proper authentication
- Weak Password Recovery Validation permits an attacker to illegally obtain, change or recover another user's password

Authorization – illegal access to applications

- Credential / Session Prediction is a method of hijacking or impersonating a user
- Insufficient Authorization permits access to sensitive content or functionality that should require more access control restrictions
- Insufficient Session Expiration permits an attacker to reuse old session credentials or session IDs for authorization
- Session Fixation attacks force a user's session ID to an explicit value

Client-side Attacks – illegal execution of foreign code

- Content Spoofing tricks a user into believing that certain content appearing on a web site is legitimate and not from an external source
- Cross-site Scripting (XSS) forces a web site to echo attacker-supplied executable code, which loads into a user's browser

Command Execution – hijacks control of web application

- Buffer Overflow attacks alter the flow of an application by overwriting parts of memory
- Format String Attack alters the flow of an application by using string formatting library features to access other memory space
- LDAP Injection attacks exploit web sites by constructing LDAP statements from user-supplied input
- OS Commanding executes operating system commands on a web site by manipulating application input
- SQL Injection constructs illegal SQL statements on a web site application from user-supplied input
- SSI Injection (also called Server-side Include) sends code into a web application, which is later executed locally by the web server
- XPath Injection constructs XPath queries from user-supplied input

Information Disclosure – shows sensitive data to attackers

- Directory Indexing is an automatic directory listing / indexing web server function that shows all files in a requested directory if the normal base file is not present
- Information Leakage occurs when a web site reveals sensitive data such as developer comments or error messages, which may aid an attacker in exploiting the system
- Path Traversal forces access to files, directories and commands that potentially reside outside the web document root directory
- Predictable Resource Location uncovers hidden web site content and functionality

Logical Attacks – interfere with application usage

- Abuse of Functionality uses a web site's own features and functionality to consume, defraud or circumvent access control mechanisms

- Denial of Service (DoS) attacks prevent a web site from serving normal user activity
- Insufficient Anti-automation is when a web site permits an attacker to automate a process that should only be performed manually
- Insufficient Process Validation permits an attacker to bypass or circumvent the intended flow of an application

There is no magic wand available for detecting web application vulnerabilities. The strategy for their detection is identical to the multi-layer approach used for security on a network. Detection and remediation of some vulnerabilities requires source code analysis, particularly for complex enterprise-scale web applications. Detection of other vulnerabilities may also require on-site penetration testing. As mentioned earlier, the most prevalent web application vulnerabilities can also be detected with an automated scanner.

An automated web application vulnerability scanner both supplements and complements manual forms of testing. It provides five key benefits:

- Lowers total cost of operations by automating repeatable testing processes
- Identifies vulnerabilities of syntax and semantics in custom web applications
- Performs authenticated crawling
- Profiles the target application
- Ensures accuracy by effective reduction of false positives and false negatives

A scanner does not have access to a web application's source code, so the only way it can detect vulnerabilities is by performing likely attacks on the target application. Time required for scanning varies, but doing a broad simulated attack on an application takes significantly longer than doing a network vulnerability scan against a single IP. A major requirement for a web application vulnerability scanner is comprehensive coverage of the target application's functionality. Incomplete coverage will cause the scanner to overlook existing vulnerabilities.

3 Phishing - the Latest Tactics and Potential Business Impact

As one of the top cybercrime ploys impacting both consumers and businesses, phishing has grown in volume and sophistication over the past several years. The down economy is providing a breeding ground for new, socially-engineered attempts to defraud unsuspecting business people and consumers. With honest money-earning avenues less available, the cybercrime ecosystem is ready with off-the-shelf phishing kits. It no longer takes a hacker to enable and commit fraud on the Internet — anyone with a motive can join in.

The potential impact on a business can be great — whether an employee or its customers have been phished or the company Web site has been compromised. Organizations need to stay current on the latest methods employed by cyber criminals and proactively take steps to prevent this type of fraud.

This fraud alert highlights the current growth and trends in today's phishing schemes, the potential impact on companies, and insight into how businesses can apply technology to protect themselves and their customers.

4 Phishing Attacks Today

Vulnerabilities in web applications are now the largest vector of enterprise security attacks. Last year – 2008, almost 55% of vulnerability disclosures affected web applications – as mentioned by an IBM official report [6].At the yearend, 72% of web application vulnerabilities had no available patch for remediation, according to that report. Articles about exploits that compromise sensitive data frequently mention causes like cross-site scripting, SQL injection, and buffer overflow.

Vulnerabilities like these fall often outside the traditional expertise of network security managers. The relative obscurity of web application vulnerabilities thus makes them useful for attacks. As many organizations have discovered, these attacks will evade traditional enterprise network defenses unless you take new precautions. To help you understand how to minimize these risks, we provide this guide as a first step to web application security. This article presents typical web application vulnerabilities, compares options for detection, and introduces the RSB-PA Web Application Scanning solution – a free on demand service that automates the available phishing reports for Romania and that will also comprise a detection mechanism for the most prevalent vulnerabilities in custom web applications.

5 Phishing Attack Models

There are five different types of generally accepted phishing attacks. The first, and most widely used during the second half of 2008 and the first quarter of 2009, is the so-called "spear phishing". It is a type of precisely targeted phishing attack; while the common phishing attacks are not discriminating network surfers the spear phishing attack targets known users of a special company, a bank or another financial institution usually.

The second type of such an attack is business services phishing. During the last year there have also been confirmed reports of two large-scale phishing attacks on the well known facebook.com socializing portal and on Yahoo.com email accounts users. Another great name of the industry that was subject to such an attack was Google; Google Ad Words users have received emails with requests for account updates, an operation redirected to a fake Ad Words interface that managed to get hold of an undisclosed number of credit card information, mostly from small and medium companies heavily relying on online advertising for attracting web traffic.

Another type of phishing attack is the so-called crisis-phishing. It is a newly arrived model and is based mostly on the fear and instability induced by the economic crisis. Phishing emails coming from a large financial institution announcing that it has recently acquired the target victim's local bank or favorite retail store seem quite in order nowadays. The large number of real mergers and acquisition activity taking place on the market today creates such an atmosphere of confusion for consumers that they are now more than ever inclined to take into account such messages. Unfortunately, phishing attacks are thriving in this type of situation.

The fourth type of phishing is in fact a mixed-model – the phishing/malware danger. To increase the odds of success some attacks combine phishing with malware for a blended attack model. A potential victim receives a phishing e-card through an e-mail that seems to be legit.

By clicking on the link inside the e-mail to receive the card, the individual is taken to a fake web location which automatically downloads a Trojan application to the victim's computer; another widely used method is to show the victim a message that indicates the need for a download of updated software, an update needed before the victim's computer can view the card.

When the victim downloads the software, it is in fact a key-logger or another security breaching application which has already been granted access and rights by the innocent user-victim.

The last, and latest, phishing attack type is based on the explosive increase in mobile phone use. Posing as a real financial institution the phishing message is using the old SMS as an alternative to e-mail in order to attempt to gain access to private and confidential information. Also known as "smishing" – from the crossing of SMS and Phishing terms – the typical message tells the mobile phone user that for example the person's bank account has been compromised or his credit card has been rendered out of service; the victim is sent to call a real phone number or access a fake website to re-enable the use of the account or credit card and once on the site or through an automated phone system, the potential victim is guided to leave its account data or card and PIN numbers.

During the 2008 year and the first quarter of 2009 there are available figures to show that despite the IT security industry's effort to reduce the phishing threat the number of such attacks is still very high and seems to be rising again.

Even if the big players of the ISP field have managed to reduce the threat of the best known and most persistent phishing groups we are still in constant danger due to the new and more sophisticated methods employed by the wrongdoers (figure 1).

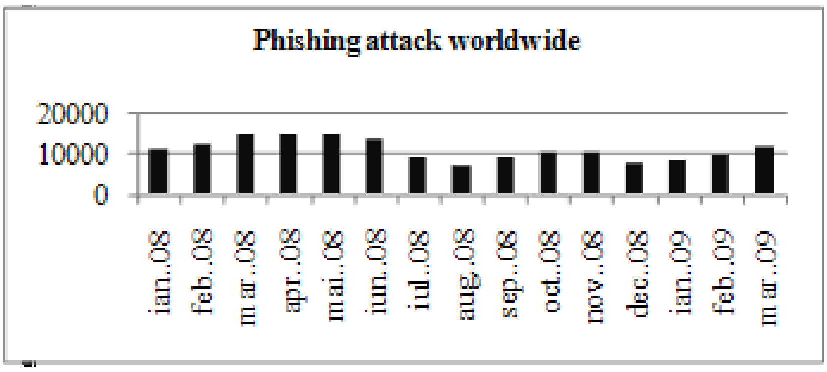

Fig. 1. Phishing attacks worldwide [5]

6 Romania's Online Security Awareness Environment

In order to help the Romanian IT environment track the latest local phishing issues, during the first quarter of 2009 we have developed a web application that works like a classic web crawler, targeted at a list of defined domains, and able to automatically retrieve phishing attacks related data from the online reports posted regularly by five of the most important names of the IT security field: Symantec, McAfee, BitDefender, RSA and APWG. The application is called RSB-PA (Romanian Security Bulletin–Phishing Attacks) for the time being and is still under development, with a future path designed to engulf two more components: for compiling virus spread information and for testing the security degree available for a certain web client accessing the application online.

Based on the compilation of these different data reported by the five sources nominated before we can produce a weekly report containing phishing attacks details strictly restricted to Romania.

During 2007 Romania experienced only 10 serious phishing attacks and in 2008 there were already 30 such attacks [2] – an increase of 3 times related to the previous year. Up to the month of June 2009 – during the January-May period of time –there were already 126 nation-wide phishing attacks, most of them being spear phishing attacks targeted at some of the largest banks in the country and on the top three mobile communications providers. Such a number can be used for projecting a whole-year number of attacks for 2009, a number around 276 attacks. These numbers show an awesome increase of about 10 times the number of attacks in 2008.

In order to understand Romania's position on the world map of phishing attacks, one of the output reports of the RSB-PA is a pie-chart graphic showing Romania's percentage of attacks, relative to the worldwide number of attacks reported by the above mentioned security companies during the relevant period of time.

Taking into account the compiled data and reanalyzing it through the RSB-PA algorithms we have also obtained an estimate of the December 2009 attacks even before the public posting of these figures by the RSB-PA "source sites". The top ten countries attacked by phishing schemes in November 2009 have the US in front with Great Britain second, followed at a great distance by Italy. The US and UK have the largest shares with 59 and 13 percent of the worldwide attacks, Italy and Romania follow with 5 and 2 percent, then we have Canada, Holland, Spain and India with 2 percent and the last one, Australia, with 1 percent; 12 percent are divided among the rest of the world.

We have to underline that these reports are not traditional ones – there is no direct oversight of the everyday attacks; we take into account all the reports from the five trusted sources mentioned above and we obtain the figures only for Romania by applying different algorithms that take into account the statistics for the previous twelve months, the number of visitors that each of the five source have during the week previous to the one of the report, the number of citations of the source website during the last twelve months and the degree of data matching between all five sources.

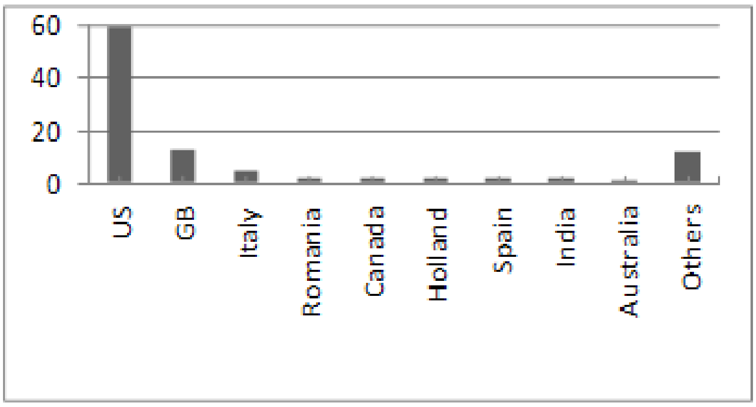

Fig. 2. Distribution of Phishing Attacks in November 2009

7 Protection through Encryption and Certificates

Customers know that any information they submit to an unsecured Web site is seriously at risk. To survive in the market, therefore, e-businesses need to incorporate SSL Certificates and the encryption technology they employ.

Encryption is the process of transforming information to make it unintelligible to all but the intended recipient. Encryption is the basis of data integrity and privacy necessary for e-commerce. Customers and business partners will submit sensitive information and transactions to your site via the Web only when they are confident that their sensitive information is secure. The solution for businesses that are serious about e-commerce is to implement a trust infrastructure based on encryption technology.

Secure Sockets Layer (SSL), the standard for Web security, is the technology used to encrypt and protect information transmitted over the Web with the ubiquitous HTTP protocol. SSL protects data in motion which can be intercepted and tampered with if sent unencrypted. Support for SSL is built into all major operating systems, Web browsers, Internet applications, and server hardware.

An SSL Certificate is an electronic file that uniquely identifies individuals and Web sites and enables encrypted communications. SSL Certificates serve as a kind of digital passport or credential. Typically the “signer” of an SSL Certificate is a Certificate Authority (CA).

The diagram on the left illustrates the process that guarantees protected communications between a Web server and a client. All exchanges of SSL Certificates occur within seconds and require no action by the consumer.

Levels of Encryption and SGC Encryption

Levels of Encryption and SGC Encryption come in various strengths, determined by the number of bits used in the encryption algorithm. The current standard is 128 bits, which is considered for all intents and purposes unbreakable at current computing speeds. Older versions of some operating systems and browsers, in certain combinations, including many Windows 2000 systems, do not support more than 40-bit or 56-bit encryption. Even the newest Window 7 operating system and its Server counterpart, Windows 2008 R2, have the possibility to use the 40-bit encryption model for connections with older systems.

Unfortunately, these levels are easily breakable today, rendering users of those operating systems and browser combinations vulnerable.

A technology called Server-Gated Cryptography (SGC), available with certain VeriSign SSL Certificates, overcomes this problem for 99.9% of Web site visitors (the rest of 0.1% represents certain older browser versions that are not capable of 128-bit encryption with any SSL certificate).

Web sites equipped with SGC “step up” to 128-bit encryption for communications with systems that normally can perform only 40- or 56-bit encryption. Therefore businesses who employ SGC SSL Certificates can guarantee the highest level of encryption available to all of their customers. VeriSign Secure Site Pro and Secure Site Pro with EV support SGC 128-bit encryption. All VeriSign SSL Certificates support up to 256-bit encryption on all connections where both the client and the server are capable of encrypting at this level.

Levels of Authentication and Trust

One of the key purposes of SSL Certificates is to help assure consumers that they are actually doing business with the Web site they believe they are accessing. Therefore CAs perform validation checks before issuing them. There are three commonly recognized categories of SSL authentication: domain authentication, organization authentication, and EV, and the differences in the level of security provided and trust engendered are vitally important. Even within a level, specific authentication processes vary from CA to CA - a key reason for choosing a widely known, respected and trusted CA.

8 Anti-Phishing Best Practices: EV-SSL

Online trust has eroded significantly in the past two years according to analyst reports, with threats of phishing and harming growing each day. In fact, a Gartner study recently reported that 20% of all consumers will not do business online at all in the near future because of security related fears. Up to now, security responses to online fraud have been quite ineffective, reactive and based on old tools which are becoming more vulnerable. Even the trusted Internet padlock has vulnerabilities that must be addressed as fraudsters become more advanced each and every month.

In response to this breakdown in online authentication a consortium of leading certification authorities and browser providers including Microsoft, Mozilla, Opera and VeriSign have teamed up to develop next generation solutions to address emerging trust threats on the Internet. The creation of EV SSL certificates was the first result of that effort and they were created to protect users from doing business with unauthenticated web merchants. Through rigorous guidelines, standards are being created that standardize online identity verification process among CA's so that consumers can know who they are doing business with.

Taking into consideration that most attacks rely on directing the users to a fake website we consider that the best option for avoiding the threat is the use of a special certificate for the accessed website. We recommend a step further than the simple use of https protocol or the implementation of SSL: the use of EV-SSL. This technology combines the versatility and encryption capabilities of the SSL with the possibility of certifying the website as legitimate with the help of a security certificate issued by a trusted CA – Certification Authority.

Despite the heavy use of encryption and secure technologies EV-SSL has another big plus from the user’s point of view: it is very simple to see it in action. All major web browsers have now the built in capability of detecting and using the EV-SSL certificates and distinguish its use by displaying a distinctive green bar in the background of the web address accessed by the user and by displaying next to the secure locker sign a text that is toggling between the name of the CA and of the client’s company or name.

The EV-SSL Certificate issuing process validates the requestor's domain control and verifies the requesting entity's legal existence and identity. The EV-SSL validation process is the most extensive and rigorous in the IT industry. This process ensures that the green trust indicator will only be awarded to trustworthy and non-fraudulent websites.

Unlike other validation processes in the SSL industry, a certification authority issuing EV-SSL Certificates cannot rely on any kind of self-reported data (such as address and phone numbers) during the validation process. This means that all data provided by a company hoping to obtain an EV SSL Certificate will be checked against reliable third-party sources.

Before such an EV-SSL certificate can be issued, three important steps are mandatory for the EV-SSL Certificate vendor:

- Confirm the existence of the Company through 3rd party sources
- Verify that the request has been made on behalf of the company
- Obtain mutual confirmation of the request between the Certificate Authority and the requesting party

Typically this is a contract that will be sent at the end of the validation process to the requesting party. The contract must be signed by an authorized person.

For all the three steps listed above, special public guidelines outline in detail what background checks are performed by all Certificate Authorities issuing EV-SSL Certificates.

A customer wishing to obtain an EV SSL Certificate must own and control the domain name that will utilize the EV-SSL Certificate. A Certificate Authority will check website registration records (Whois database) or may ask the customer to make a change to the website under the domain name.

The Certification Authority must verify that the individual requesting the certificate is acting as a legitimate agent for the requesting company.

One way that a Certificate Authority may verify this data is by contacting the requesting company's human resource department.

The Certificate Authority will also verify the identity of the contract signer (in most cases this will be a management level person). Usually this is verified with written documentation.

A Certificate Authority will check to make sure that the business is legally recognized and that the formal name matches the official Government records. In cases where a trading name is used, the Certificate Authority must verify any alternative names that differ from the legal name of the customer in qualified databases.

The Certification Authority is required to cross-check the address listed in the certificate application against a qualified government database, or an international recognized one if the request for the certificate comes from another country and the company is part of an international organization.

If the listed address cannot be verified by consulting the government database, an on-site visit may be necessary to investigate the discrepancy. Investigators may need to take photos of business operations or speak with company personal.

The Certificate Authority will confirm that the telephone number listed on the certificate application is the primary telephone number for the requesting organization. This is accomplished by calling the number directly or by checking phone directory listings.

Despite the advanced capabilities to copy legitimate websites, without the user’s EV-SSL Certificate there is no way to display its name on the address bar because the information shown there is outside of webpage control; one cannot obtain somebody else’s legitimate EV-SSL Certificates because of the very rigorous and stringent authentication process.

9 Conclusion

Besides implementing the EV-SSL, the IT companies and the online businesses should continue to educate their customers and bring them the knowledge required by the 21st century society and related to safe network use and practices.

All it specialists of this field of “web security" should spread around the information related to recognizing the most usual signs of phishing: a certain degree misspellings, generic salutation formulae instead of clear and personalized ones, urgent "must" deadlines for acting in a certain manner, account status threats, requests for the user's personal data and information or fake domain names and links. They should also educate users and help them understand how to recognize a good, valid and secure site before rushing in and providing personal and sensitive information to a certain internet webpage:

- check the URL address for its starting point: this should be HTTPS
- look for the "green bar" related to the EV-SSL presence
- click the secure locker to the certificate of the website

As a last conclusion, good user education is a key component for building the trust necessary to overcome the phishing fears. By the use of up-to-date security solutions on a website any company can start capitalizing on this trust and then gain a real and tangible benefit from investing resources into the secure development of its online presence.

References

[1] G. Aaron and R. Rasmussen, *Global Phishing Survey: Trends and Domain Name Use in 2H2008*, 2009, [Online], Available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf

[2] C. Cosoi. Prevenirea pericolelor IT şi non-IT (securitate) – Preventing IT and non-IT threats (security), 2008, [Online]. Available at: http://www.calendarevenimente.ro/detalii.php?ev=6088

[3] C. Kasten. My EV SSL Journey, 2008, [Online], Available at: http://www.solo-technology.com/blog/2008/08/21/my-first-ev-ssl-journey

[4] M. O'Donnell. Counterfeiting & Spear Phishing - Growth Scams Of 2009, 2009, [Online], Available at: http://www.infonews.co.nz/news.cfm?l=1&t=164&id=33971

[5] U. Rivner, *RSA Online Fraud Report May 2009*, 2009, [Online], Available at: http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0509.pdf

[6] IBM Corporation, *ISS X-Force 2008 Trend & Risk Report*, 2008, [Online], Available at: http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf

Ion LUNGU is a Professor at the Economic Informatics Department at the Faculty of Cybernetics, Statistics and Economic Informatics from the Academy of Economic Studies of Bucharest. He has graduated the Faculty of Economic Cybernetics in 1974, holds a PhD diploma in Economics from 1983 and, starting with 1999 is a PhD coordinator in the field of Economic Informatics. He is a CNCSIS expert evaluator and member of the scientific board for the ISI indexed journal Economic Computation and Economic Cybernetics Studies and Research. He is also a member of INFOREC professional association and honorific member of Economic Independence academic association. In 2005 he founded the master program Databases for Business Support (classic and online), who's manager he is. His fields of interest include: Databases, Design of Economic Information Systems, Database Management Systems, Decision Support Systems, Executive Information Systems.

Alexandru TĂBUŞCĂ has a solid background in computer science and is interested in IT security issues and web technologies. He has graduated the Faculty of Computer Science for Business Management from the Romanian-American University in Bucharest in 2000 and obtained the Diploma from the Faculty of Economic Cybernetics, Statistics and Informatics from the Bucharest Academy of Economic Studies in 2001. In 2004 he was decorated with the “Educational Merit” Medal – Third Class, awarded by the Orders Office of the Romanian Presidential Administration. He has graduated the Economic Informatics Master Program from the Romanian-American University in 2005. He is currently preparing for the final public presentation of his doctoral thesis in Economic Informatics at the Academy of Economic Studies. Other fields of interest include object oriented programming in Java, network design and architecture, hardware and software encryption systems, web design and history.