Protection of National Cyber Security: Awareness & Education

Yılmaz VURAL
Hacettepe University
Computer Engineering Department
06800 Ankara TURKEY
+90 (312) 297 7500
yvural@hacettepe.edu.tr

Murat AYDOS
Hacettepe University
Computer Engineering Department
06800 Ankara TURKEY
+90 (312) 297 7500
maydos@hacettepe.edu.tr

Mehmet TEKEREK
Kahramanmaraş Sütçüimam
University, CEIT Department
46050 Kahramanmaraş TURKEY
+90 (344) 280 1310
tekerek@ksu.edu.tr

ABSTRACT

It is identified that one of the greatest threats against security in the next coming ten years will be cold cyber wars against information systems between countries. National information systems utilize the information technology infrastructure of enterprises in order to satisfy personal or enterprise needs. In the past years, attacks were taking place with no discrimination of targets, however in the recent years; attacks are organized, deliberate and pointed towards national information systems. Personal and enterprise level information security must be established in order to avoid information security threats that try to hamper or even destroy national information security, cause tangible and intangible damages on individuals and enterprises.

In order to reduce the impact of such cyber threats to minimum at the national level, there are necessary critical enterprise and personal security precautions to be taken. The establishment of the enterprise and personal information security which form the stages of establishing national information security at highest level and development of a national security policy are among the first things that need to be done.

In this paper, the strategic national information systems are identified, then personal and enterprise information security that are important stages in providing security for national information systems are described. The necessary security tests and the importance of education and awareness are discussed in the following section. Finally, evaluations have been performed on national information security and proposals have been put forward.

Categories and Subject Descriptors

D.4.6 [Security and Protection (K.6.5)]: - *Access controls, authentication, cryptographic controls, information flow controls, invasive software (e.g., viruses, worms, and Trojan horses), security kernels, and verification*

General Terms

Information Security, Homeland Security

Keywords

Information Security, E-government, Up-to-date vulnerabilities

1. INTRODUCTION

While our life gets easier as a result of the use of information systems becoming widespread at the enterprise and personal level, the need increases for the information systems which are highly secured [1]. If the value of the information which is maintained by the increasing number of applications that are widely used throughout the country and communicate through network centric information systems is considered, the importance of establishing information security will be better understood. Besides, if it is considered that newly developed applications bring along new security threats, it will be better evalauated that the establishment of information security is getting more difficult day by day.

The interaction between network centric information systems of public and private enterprises is increasing in time and these systems are forming the infrastructure of national information systems. Within or between the enterprises, national information systems enable the sharing and utilization of strategic national information and therefore establishing the security of these systems at highest level is critical for national security.

It is necessary to protect the national information systems at highest level that include personally and organizationally critical information against foreign intelligence or terrorist cyber attacks. The threats against the national information security are not only on electronic platforms. As a result of natural or undesired events such as human errors, fire, flood, earthquakes, terrorist attacks or sabotage, information and information systems can be partially or completely damaged. Besides unprotection, the incorrect identification of protection level as well as not taking necessary security precautions brings along other significant problems such as additional cost, low performance or unproductivity.

Nowadays, almost every day, we talk about the security breaches and violations in electronic environments. As a result of one of those security breaches, being a significant example for national information security, “Distributed service denial attacks against the national information systems of Estonia”, the public, bank and media internet sites in Estonia having 1.3 million population, have been down and everyday activities were greatly reduced, nearly stopped, due to large scale, coordinated and continous attacks originated through Russia from hundreds of thousands of computers [2]. This attack has been noted in history as the first cold cyber war between governments.

In a report that is prepared through the end of 2007 by Internet Security Company McAfee, it is identified that one of the greatest threats against security in the next coming ten years will be cold cyber wars against information systems between countries. In the report it is indicated that approximately 120 countries have developed solutions to utilize internet for financial markets, governmental computer systems or public services and intelligence agencies continuously examining other governments' national information systems in order to develop new techniques to reveal their weak points [3-4].

In order to reduce the impact of such cyber threats to minumum at the national level, there are necessary critical enterprise and personal security precautions to be taken. The establishment of the enterprise and personal information security which form the stages of establislishing national information security at highest level and development of a national security policy are among the first things that need to be done.

In this paper, national information systems which include strategic national information are explained, personal and enterprise information security that are important stages in providing security for national information systems are described and security tests and the importance of education is discussed in the following sections. Finally, evaluations have been performed on national information security and proposals have been put forward.

2. NATONAL INFORMATION SYSTEMS

Information indicates complete data that is given a meaning by individuals or enterprises as a result of the activities such as solving a problem, beginning or finalizing an activity. The origin of word "information", is the Latin word "informare" that means to give shape or form to something [5]. In its dictionary meaning information is defined as "all kinds of fact, knowledge and understanding gained through learning, research and observation" [6]. Information systems consist of components such as harwdware, software, communicatin technologies and people. As information is produced, processed, transferred and stored through information systems, security threats and necessary precautions have become increasingly different.

National information systems are defined as systems that are substantially national in geographic scope (i.e., multistate); are organized by government or private organizations or groups to collect, store, manipulate, and disseminate information about persons and/or institutions; and are in some significant manner based on computers and related information and communication technology [7]. By means of national information systems it has become possible independent of location to access and share information that is produced, processed, transferred and stored in network centric environments. Population Citizenship Administration MERNİS, Finance Ministry Internet Tax Admininstration, Social Security Organization Information System, Meteorology Information Services, Geographical Information Systems and Bank Information Systems can be examples of our national information systems.

The activities continue for National Information System that will incorporate our national information systems and enable their interoperability. National Information System is the group of national information systems having the objective of correlating, sharing and management of strategic information within the related organizations towards public administration [8]. With the establishment of National Information Systems, enterprise information systems will be capable of interoperability in a network centric environment through a system of systems approach.

System of systems is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to obtain a new, more complex, 'meta-system' which offers more functionality and performance than simply the sum of the constituent systems [9]. The best example to the system of systems is Internet. Internet has developed in years very extensively and now available throughout the world becoming the network of information systems.

Above and beyond the many capabilities that will be gained by forming National Information System through system of systems approach, problems in security, performance and management should be considered and resolved. For the resolution of all security related problems, information assurance comes into prominence.

Information assurance (IA) is the practice of managing information-related risks. More specifically, IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These goals are relevant whether the information are in storage, processing, or transit, and whether threatened by malice or accident. In other words, IA is the process of ensuring that authorized users have access to authorized information at the authorized time [10]. By means of information assurance, the integrity of network and information infrastructure of national information systems will be possible. Information Assurance must be applied to all national information systems that interoperate. In order to establish the national information security at highest level, it is necessary to establish enterprise information security nationwide at adequate protection levels. Therefore, in the following section, the establishment of enterprise information security at highest level is explained.

3. ENTERPRISE INFORMATION SECURITY

Information is a critical asset to the operation and perhaps even the survival of organizations. Enterprise information is now globally accepted as being a vital asset for most organizations and businesses. As such, the confidentiality, integrity, and availability of vital corporate and customer information may be essential to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image [11].

Enterprise information security defines enterprise information as an asset, which adds value to an organization and consequently needs to be adequately protected. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or communicated in conversation. Additionally, information security is defined as the

establishment of the integrity and secure delivery of information confidentially, without being damaged or changed and without being acquired by third parties from the information sender to the receiver, in an environment where the access to information is continuous [12]. Enterprise information security is to reveal vulnerabilities through the identification of enterprise information assests and to take necessary precautions performing security analyses with the objective of protection against threats and dange and to manage security processes according to the related standards [13].

Enterprise Information Security is an important stage in order to establish national information security. It is not possible to achieve national information security without the establishment of enterprise information security. For the establishment, planning, design, development, operation, tracking, controlling, maintaneance and improvement of enterprise information security, business risk approach An information security management system (ISMS) is, as the name suggests, a set of policies concerned with information security management [14]. The key concept of ISMS is for an organization to design, implement and maintain a coherent suite of processes and systems for effectively managing information accessibility, thus ensuring the confidentiality, integrity and availability of information assets and minimizing information security risks.

In order to be able to protect important enterprise information and information systems, to minimalize risks and to establish continuity, it is necessary to put EISMS into practice in enterprises. The establishment of EISMS implies actualization of a series of audits complementing each other such as identification of potential risks and threats, development of security policies, control of audits, and applications, development of appropriate methods, organizational structuring and providing software/hardware functions.

It is not possible to establish enterprise information security with only technical precautions (firewalls, attack identification systems, antivirus software, antispyware software, encryption, etc.). EISMS is a management system that incorporates people, processes and information systems and supported by the upper management. Enterprise information security consists of complex processes that are difficult to manage and are impacted by a multiple of factors such as people, education and technology.

Enterprise Information Security should not only be evaluated as a technology problem but also as a people and management problem [15]. If the reasons behind the security violations in the enterprises due to employee and management errors are examined, the common problem of employees at different organizational levels being end-users or managers, is observed to be the lack of education and awareness. The support of the upper management level developing organizational strategic goals is very important in order to establish enterprise information security. It is necessary to form an enterprise information security unit so as to enable administrative and financial decision making for the establishment of information security. Necessary security related strategic decisions have to be taken by this unit in time and in appropriate manner. The formation of enterprise information security unit by the management and its effective operation is a significant indication of management support for and ownership of enterprise information security.

The standardization activities continue in our country and in the world in order to develop, manage and configure processes for establishment of enterprise information security at highest level. Cyber security standards are security standards which enable organizations to practice safe security techniques in order to minimize the number of successful cyber security attacks. These guides provide general outlines as well as specific techniques for implementing cyber security. One of the most widely used security standards today is ISO/IEC 27002 which started in 1995. This standard consists of two basic parts. BS 7799 part 1 and BS 7799 part 2 both of which were created by (British Standards Institute) BSI. Recently this standard has become ISO 27001. [16].

Despite being an important stage, establishment of enterprise information security is not sufficient for establishment of national information security only by itself. In order to establish the national information security at highest level, the security of end user information, i.e. personal information security needs to be established as well. For this reason, in the following section, explanations have been provided for the establishment of personal security at highest level.

4. HUMAN FACTORS

It is indicated in the reports, questionnaires, books and articles that are related with information security and are examined in the scope of this paper that the weakest link in establishment of information security is the human factor [17-23].

Despite all the technological security precautions taken, the abuse of weaknesses resulting from human factor will lead to information security violations. These violations will cause problems that are critical for national information security.

The errors due to human factor that threathen personal information security as well as necessary precautions to be taken are summarized below in subheadings.

Violation of Security Policies: Every user who has access rights to the information in information systems need to abide by innformatio n security policies. Security policies are violated by end users most of the time intentionally or unintentionally. It is identified that the major reasons for the violation of security policies are user habits, unapplicable sanctions and lack of awareness. In order to avoid security violations, the users need to be trained in information security topics and security policies need to consist of statements that are applicable.

Information Exchange: People exchange important information usually unacquainted with unfamiliar persons. No user shall exchange information with people whose identity is unknown regardless of the means (e-mail, telephone, telefax, face-to-face, etc.). It must never be forgotten that it is possible to breach security controls with the information acquired from an enterprise personnel without any use of technology at all. There are more and more examples each day that little pieces of information that seemed to be insignificant at the beginning, when combined

together can turn into a serious security hole. In order to avoid information exchange with unknown persons, it is necessary to train the end users especially in the area of social engineering.

Writing passwords on papers: Encryption policies enforce the utilization of passwords that are hard to be broken and the change of these passwords regularly by the users. The encryption power is directly proportional to the complexity of characters that are used in a password. With the application of powerful encryption policies, the problem of remembering those passwords by the users arises. Under this circumstance, in order to be able to remember their passwords, users write their passwords on a paper at their disposal. This situation leads to a security violation of discovery and abuse of the password by another person with malicious intentions. In order to avoid such situations, users need to get trained in selection and recollection of passwords.

The utilization of unreliable software: Unreliable software is software that is illegally copied or downloaded from unreliable internet sites without appropriate licenses and can contain viruses, trojans, key recording and all other kinds of malicious software. Unreliable software keeps the recordings of visited web sites and send this information to others, opens up undesired advertisement popups, can send personal files in computer system to others, reduces the computer performance and exploits internet connectivity. Many security violations take place as a result of utilization of unreliable software. In order to avoid such violations, the users need to get trained in what unreliable software is and how to evade such software.

Establishment of the physical security of computers: When the users leave their computers without taking any protection measure, people with malicious intentions making use of this situation utilize the computer for maleficient purposes and security violations take place. Taking advantage of physical security vulnerability, the person with malicious intentions can email files containing confidential information to other parties, delete or change the information on the computer system and can perform other actions within the user rights of that user. For the establishment of the physical security of computers, it is necessary to raise the awareness of users in this topic; at least the utilization of password protected screen savers must be considered to minimize the risk of such physical attacks to computers.

Starting up computers with administrative rights: Users utilize computers within the enterprise that are allocated to their use with the accounts that have administrative rights without any limitations. This situation leads to the violation of the principle of least privilege which is one of the fundamental principles in establishment of information security. Starting up a computer with an account that has administrative rights will exacerbate the impact of security violations due to the user account that is in use having administrative rights at the time of a security violation. In order to reduce the impact of such violations, it is necessary to define accounts with limited rights that satisfy the needs of the users and it shall be mandatory for the users to start their sessions with these accounts. In addition to this preventive measure, it is necessary to give encouraging and informative trainings to the users explaining inappropriateness of starting sessions with the accounts that have administirative rights and to make them use the accounts with limited rights.

E-mail utilization without awareness: E-mail is one of the most common means of communication among employees. As malicious software spreads usually through e-mails, the utilization of e-mails with awareness has become more important. Inadvertent uses of email cause security violations. It is necessary to raise the awareness of and educate the users about the important precautions that can be taken during the use of e-mails, such as not opening up e-mails from unknown senders, scanning e-mail attachments for viruses, not sharing personal confidential information (internet bank accounts, identity card data, user account information, etc.) via e-mail. As a result of these, the weaknesses due to use of emails will be minimized.

Generally speaking, education has an important role in eliminating the vulnerabilities originating from human factor which is the weakest link in the establishment of information security. The importance of education is examined in detail in the following section.

5. AWARENESS AND EDUCATION

In order to establish national information security, different methods need to be used to raise awareness of and provide education for different users who can utilize national information systems at different levels. These methods can include creating awareness by holding meetings, organizing trainings over the web and sending notifications, announcements, seminars, newsletters or security related posters via email.

Although the security risk due to human factor can not be completely eliminated, information security trainings that are well planned can reduce risk to an acceptable level. It is critical in order to minimize security vulnerabilities due to human factor that groups of people with different backgrounds understand their responsibility and fulfill their obligations of protecting information and information resources.

The major objective of information security trainings is to educate people about their obligations and responsibilities necessary for establishing confidentiality, integrity and accessibility of information resources. With these trainings, it is essential to train people not only on how information is protected but also why it is necessary to protect information. Employees must clearly understand the impact of their errors on national information security. Raising the awareness of users will help to reduce the cost impact of security violations and provide a well balanced control over the complete information resources of the enterprise.

The purpose of security awareness is to focus attention on security, creating sensitivity to the threats and vulnerabilities of computer systems and recognition of the need to protect data and national information systems [24]. Messages to create security awareness must be simple and clear and the trainings for raising awareness should be in plain format for quick and easy understanding of groups of people from different backgrounds.

In most of the enterprises, the application of security enforcements is delayed because necessary security limitations are not inline with user habits. When security enforcements are delayed, each user develops different usage behaviors which makes security awareness education difficult as well as creates

user resistance against security enforcements. Hence, it is not only sufficient to train users but also necessary to get rid of old habits.

According to users, the enterprise has worked very well up to date without security enforcements and did not encounter any problems. New security enforcements seem to be inconvenient and unnecessary changes. The trainings for creating awareness must be fluent and enjoyable and be prepared to address elimination of old habits along with providing security related information.

The research undertaken within the scope of this paper indicated that there were no security awareness programs in most of the enterprises or the trainings failed to educate users on why information security is important in those enterprises which had these programs. Successful trainings must address the question "why" convincingly for users. A successful training must result in that users own and are willing to apply the security policy. Most of the users are ignorant of the significance of protecting information and information resources. A well designed and performed awareness and education activity will help strengthening the human factor which is the weakest link of the security chain.

After the enterprise and personal information security stages for the establishment of national information security, the education aspect has been emphasized that minimizes the vulnerabilities due to human factor. In the following section, security tests have been explained as they are necessary to control the applicability of national information security processes.

6. SECURITY TESTS

A complete examination of the factors that affect information security from attacker's point of view and identification of corrections and hardenings in order to detect and eliminate vulnerabilities summarize the importance of security tests for establishment of national information security.

Security testing is an important early warning system that is utilized to reveal the system vulnerabilities and identify counter measures before an attack on information systems takes place. For successful security tests, it is necessary to take the weight of factors that have impact on the security of information systems into account and to develop different scenarios particular to different systems. The scenarios developed for security tests will be different according to the technology utilized, the information level of users, the required level of information security and the characteristics of information security components.

Non technical tests must be carried out in addition to technical tests which identify information security violations in a controlled manner. Social engineering tests are the most important of such non technical tests. Social engineering is the act of manipulating people into performing actions or divulging confidential information [25]. Different methods are utilized to perform social engineering tests. The most common method is imitation and persuasion via a telephone call.

There are multiple open source standards and guidelines (OSSTMM, NIST, OWASP, etc.) to perform security tests. Use of these standards during security testing is important for tests' success.

With this research, it is identified that security tests are not common among enterprises in our country and their importance in establishing enterprise information security is not evaluated sufficiently. This circumstance is an indication that the substantial contribution of security tests to the enterprise security in terms of raising awareness and improving the security level of the enterprises is not known adqueately and not given the necessary importance.

7. RESULTS

National information systems, e-government applications utilize the information technology infrastructure of enterprises in order to satisfy personal or enterprise needs. In the past years, attacks were taking place with no discrimination of targets, however in the recent years; attacks are organized, deliberate and pointed towards national information systems. Personal and enterprise level information security must be established in order to avoid information security threats that try to hamper or even destroy national information security, cause tangible and intangible damages on individuals and enterprises. Information security processes of national information systems must be managed according to international standards.

National information systems contain critical information for countries. Irredeemable situations can take place for the countries if critical information is subject o cyber attacks due to vulnerabilities in information security. Unauthorized, untimely opening a dam's shutters, hindrance of civil or military communication systems, destruction of electrical or natural gas power plants, bringing down the information systems of banking, education and health sectors can be examples of information system oriented attacks that threaten national security. In order to provide protection against these types of attacks, national security policies must be developed and national information security must be established accordingly.

Losses caused by the attacks against confidentiality, integrity and accessibility of information are serious and can not be compensated. It is impossible to eliminate all the losses completely. However, it is possible to minimize them by carrying out security tests. It is necessary that the security tests of national information systems are performed according to contemporary national security policy developed by a national authority. State funded centers to perform security tests free of charge must be formed and national software applications for security tests must be developed and used.

When "Your security is as much as your weakest link" principle is considered, in order to eliminate the vulnerabilities due to human factor which is the weakest link in national information security chain, information security education and awareness should be provided at each level of education from the elementary schools to the universities. In order to realize this, a great part of the mission falls especially to non governmental organizations, Ministry of National Education and universities.

Identification of the cyber attacks that threaten national security has an important role in development of national strategies in order to establish information security. When the organized attacks against the information systems are examined, it has been identified that the attacks are carried out using advanced techniques and are widespread from personal to national level. In order to establish national information security, the types of attacks need to be monitored, the advanced techniques used by the attackers must be identified, and the security holes described in related research, reports and acvities in our country and in the world must be handled and eliminated in time.

Finally, when it is considered that the activities and precautions necessary for establishment of national information security are not sufficient, personal and enterprise level information security awareness and education has not taken place adequately in our society and that the establishment of national information security in our country is not performed at highest level, it is necessary to take the key aspects presented in this paper into account and carry out the proposals.

8. REFERENCES

[1] Thow-Chang, L., Siew-Mun, K., and Foo, A., "Information Security Management Systems and Standards" Synthesis Journal, 2(2):5, 8 (2001).

[2] Sandham, D., "News", Communications Engineer Publication 5(4):3-8, (2008).

[3] İnternet: "McAfee Virtual Criminology Report" http://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf (02.02.2016)

[4] Vural, Y., "Kurumsal Bilgi Güvenliği ve Sızma Testleri", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 15-20, (2007).

[5] Rocha, L. M., Schnell, S., "The Nature of Information-Lecture Notes", Indiana University, Bloomington, 1, (2007).

[6] İnternet: Türk Dil Kurumu "Güncel Türkçe Sözlük" http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=bilgi

[7] İnternet: "National Information Systems Advisory Panel-Computer-Based National Information Systems" http://govinfo.library.unt.edu/ota/Ota_5/DATA/1981/8109.PDF (15.05.2009).

[8] İnternet: "Türkiye Ulusal Bilgi Sistemi:Genel Esaslar" www.hssgm.gov.tr/stratejikyonetim/egitim_dokumanlari/turkiye_ulusal_bilgi_sistemi_esaslari.pdf (15.05.2009)

[9] İnternet: Wikipedia, "System of Systems", http://en.wikipedia.org/w iki/System_of_systems (15.05.2009)

[10] İnternet: Wikipedia, "Information Assurance", http://en.wikipedia.org/wiki/Information_assurance (15.05.2009)

[11] Bhatt, G. D., "Knowledge Management in Organizations: Examining the Interaction between Technologies, Techniques and People", Journal of Knowledge Management, 5 (1):71, (2001)

[12] Vural, Y., Sağıroğlu, Ş., Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, ISC Turkey Uluslararası Katılımlı Bilgi Güvenligi ve Kriptoloji Konferansi, Ankara, 191-199, Aralık 2007

[13] Vural, Y., Sağıroğlu, Ş., Gazi Üniv. Müh. Mim. Fak. Der. 23(2), 507-522, (2008)

[14] Türk Standardları Enstitüsü, "Bilgi güvenliği yönetim sistemleri", TSE-TS 1779- 2, Ankara, 3, (2005).

[15] Mitnick, K. D., Simon, L. W., Wozniak, S., "The Art of Deception: Controlling the Human Element of Security", Wiley Publishing, New York, 17-18 (2003)

[16] İnternet: Wikipedia, "ISO/IEC 27001", http://en.wikipedia.org/wiki/ISO_27001 (15.05.2009)

[17] İnternet: CERT "Historical Statistics" http://www.cert.org/stats/historical.html (09.11.2008)

[18] Dunlevy, J. C., "Information Security Strategies: A New Perspective", CERT, Pittsburgh, 15, (2006)

[19] Internet: World Stats "Top 20 Countries With The Highest Number Of Internet Users" http://www.internetworldstats.com/top20.htm (15.05.2009)

[20] Symantec Corp., "Symantec Internet Security Threat Report Trends for July–December 07" Symantec Volume XII, Cupertino, 24-64 (2008).

[21] Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R., "CSI/FBI, Computer Crime and Security Survey", FBI Computer Security Institute, 1- 26, (2005).

[22] Koç.net Haberleşme Teknolojileri ve İletişim Hizmetleri A.Ş., "Türkiye İnternet Güvenliği Araştırma Sonuçları 2005", Koç.net, İstanbul, 5- 12, (2005)

[23] İnternet: "Information Security Awareness" http://www.massachusetts.edu/SecurityAwareness/securityawareness.html (15.05.2009)

[24] Morales, L.; Dark, M., "Information Security Education and Foundational Research", System Sciences, HICSS 2007. 40th Annual Hawaii International Conference, Hawaii, 269 (2007).

[25] İnternet: Wikipedia, "Social Engineering", http://en.wikipedia.org/wiki/Social_engineering_(security) (15.05.2009)