NATIONAL CYBER SECURITY EXERCISE 2011
FINAL REPORT

25-28 January 2011

ISBN: 978-605-62506-1-3

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

TÜBİTAK

ULUSAL SİBER GÜVENLİK TATBİKATI • 2011 •

U S G T

content

abbreviatons

APCERT	Asia Pacific Computer Emergency Response Team
ISMS	Information Security Management System
BİLGEM	Center of Research for Advanced Technologies of Informatics and Information Security
BTK	Information and Communication Technologies Authority of Turkey
CERT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
ECA	Electronic Communications Act
IDS	Intrusion Detection Systems
IP	Internet Protocol
ITU	International Telecommunication Union
ISP	Internet Service Provider
NCDEX	NATO Cyber Defense Exercise
NGO	Non-governmental Organization
NCSE	National Cyber Security Exercise
TOBB	Turkish Union of Chambers and Exchange Commodities
TÜBİTAK	The Scientific and Technological Research Council of Turkey
UEKAE	National Research Institute of Electronics and Cryptology

EXECUTIVE SUMMARY

National Cyber Security Exercise (NCSE) - 2011 was carried out in 25-28 January 2011 with the participation of 41 public, private and non-governmental organizations (NGOs) including judicial and law enforcement agencies and various ministries as well as the ones from a diverse set of sectors such as finance, information technology and communication (ICT), education, defense and health. (See Figure 1). Six of those organizations participated in the exercise as observers. Approximately 200 officers who are experts in the fields of ICT, law and public relations from the participatory organizations attended the exercise. In NSCE – 2011, not only the technical competence but also the intra and inter organizational coordination capabilities of the participants were evaluated by measuring their responses to the cyber attacks in both the real and the simulation environment.

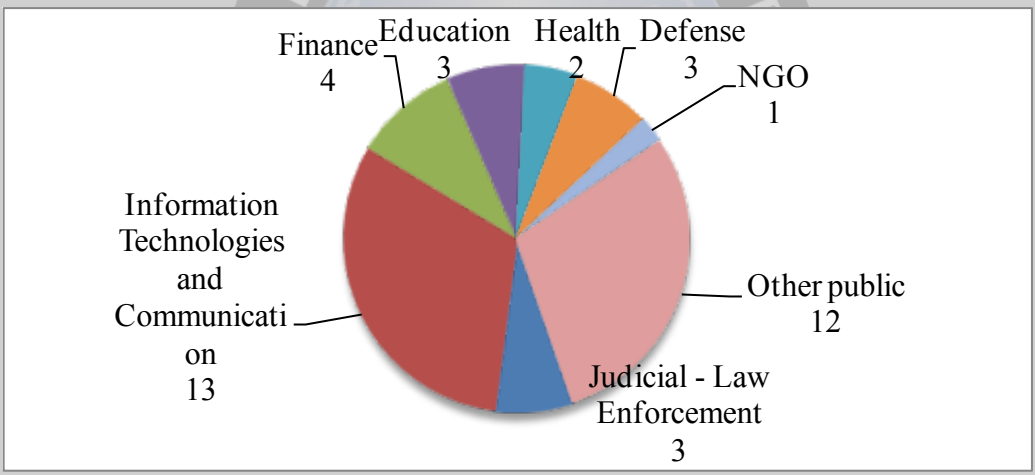

Figure 1. Sectoral Profile of the Participatory Organizations

In the first two days of NCSE - 2011 carried out in 25-26 January 2011, the participants joined the exercise in their own premises. The last two days of NCSE - 2011 were collectively fulfilled at the Conference Hall of TOBB Economy and Technology University.

During NCSE – 2011, the second national cyber security exercise held in Turkey, both real attacks and written scenarios were actualized in order to determine the technical competence of the participants, and to have the

participants gain response experience in case of possible attacks.

The findings reached at the end of the written scenarios and the real attacks carried out within the context of NCSE – 2011 are summarized below. More detailed information is provided in the second part of the report.

Finding 1. Lack of Information Security Management Systems:

It was detected that some of the participants did not have an Information Security Management System (ISMS) established, any written policies, especially information security policy, procedures and instructions prepared or any risk analysis done. It was also observed that the participants did not have an information security culture with regard to dealing with information security vulnerabilities, and how to determine the corrective and preventive actions in order not to face any cases similar to the ones in the exercise.

Finding 2. Technical Incompetence of the System Administrators:

In some of the participatory organizations, it was determined that the system administrators did not have sufficient technical knowledge to deal with a problem in the system; therefore the problem-solving time was longer than it should be.

Finding 3. Lack of Intrusion Detection Systems and Processes:

It was observed that IDSs were not used by some of the participants with the aim of taking precaution against the regular attacks. On the other hand, as to the participants having IDSs, it was noticed that the logs produced by those systems were not examined effectively; therefore difficulties were experienced in detecting the attacks.

Finding 4. Lack of Awareness about Social Engineering Attacks:

It was detected that some of the participants searched for only technical solutions to security events, and ignored the human factor, which is the most important link in security chain.

It was also observed that in some of the participants, the personnel were not provided with regular awareness training regarding social engineering attacks, and information security reminder methods like sending warning e-mails to the users regularly and hanging information security posters at certain places of the workplace were not used effectively in order to

prevent this kind of attacks. In addition, it was noticed no periodic social engineering tests were conducted with the purpose of increasing resilience of the personnel against such attacks.

Finding 5. Outdated Antivirus Systems:

It was determined that the signature files of central antivirus servers were not regularly updated; therefore the signature files of antivirus software, installed on end units and updated from the central antivirus servers, were not periodically updated, either.

Finding 6. Incompetency of System Administrators in terms of Security:

It was observed that the system administrators in some of the participatory organizations did not have necessary competence for information security; also the participants were not in contact with security interest groups, other specialist security forums and professional associations.

Finding 7. Lack of Intra-Organizational Coordination:

It was detected that the coordination among the internal units in most of the participants was insufficient, some units were not provided with substitute staff. Therefore, in case of an information security event, the necessary steps could not be taken, and either no contact or late contact with the corresponding authorities could be made.

Finding 8. Lack of Access Control Policies:

Some of the participants did not have an access control policy that uses business and security requirements as base for access. As a result of this, the staff could gain unauthorized access to irrelevant information and services .

Finding 9. Ignoring Security at the System Design Stage:

It was noticed that some participants had not consider security as a main design principle at the system design stage; which caused security breaches to occur and complicated effective response against the security cases.

Finding 10. Risks arising from Wireless Networks:

It was observed that some of the participants could not detect the unauthorized wireless access points installed by the attackers; from which the personnel might get service.

Finding 11. Lack of Business Continuity Plans:

It was detected that some of the participants did not have a business continuity plan established for preventing business interruption and maintaining business processes in case of an information security incident causing system interruption.

Finding 12. Inability to Detect Port Scan Attacks:

It was noticed that some of the participants could not detect "Port Scan" attacks against their information systems connected to Internet.

Finding 13. Unfavorable Results of Distributed Denial of Service (DDoS) Attacks:

It was detected that as a result of DDoS attacks, most of the participants experienced a business interruption; the ones that did not have business interruption were the ones that purchased service from their Internet Service Providers (ISS) in order to be protected from this kind of attacks. This reveals the importance of inter-organizational communication, cooperation and coordination for enabling information security.

Finding 14. Vulnerabilities in the Web Applications:

Certain vulnerabilities were detected in the web applications running on the participants' information systems connected to Internet. The participants considering security as an essential requirement during application development and having their applications checked by independent government agencies and organizations were noticed to have respectively less vulnerabilities in their web applications.

Finding 15. Inability to Analyze the Log Files Properly:

Some of the participants were observed not to be able to determine when, how and by whom the attack was carried out by means of analyzing the

attack log files formed during the attacks made within the context of the exercise. The participants which had a special information security unit were observed to be respectively more successful.

Evaluating these findings generally, it is seen that comprehensive studies should be made in the fields of information security management systems, business continuity, human resources, intra and inter organizational coordination; also the efficiency of ongoing researches should be increased in order to enhance cyber security in Turkey.

1. THE EXERCISE NEED AND THE RELEVANT GOVERNMENT AGENCIES AND ORGANIZATIONS

Information Society in the World and Security

More and more people use information systems every day in the process of transformation to information society and become more addicted to these systems. Many systems such as electricity, gas, water, communication and transportation, highway, railway and airway are run by information technology components. All these developments have carried the information systems to a rather critical point and made them values that should be protected.

Many studies and regulations about cyber security are made in the world and Turkey. These studies and arrangements are based on the concept of avoiding cyber threats and protecting the users. 11 main activity fields were determined at the end of World Summit on the Information Society, arranged by International Telecommunication Union (ITU) and of which the first stage was held in Geneva in December 2003 and the second stage was held in Tunis in November 2005. One of the aforesaid main activity fields, the task of "Establishing Privacy and Security in the Use of Information and Communication Technologies", was given to ITU by the international society. ITU has made researches about this task since 2005.

It is noticed that the exercises carried out within the national and international context take an important place in the studies related to cyber security in the world. By these exercises, inter organizational coordination capabilities in addition to organizational statuses on cyber security are evaluated and improvement studies are performed under the light of findings.

Studies in Turkey

In this part, the past and ongoing studies about information security in Turkey are summarized in chronological order.

The 2006-2010 Information Society Strategy and Annexed Action Plan was adopted by High Planning Council with the decision numbered 2006/38 and published on the Official Gazette dated 28/07/2006. It was prepared within the framework of e-Transformation Turkey Project carried out with an intent to coordinate the process of Turkey's transformation into an

information society. With the action item numbered 88 and entitled "National Information Systems Security Program" in the 2006-2010 Information Society Action Plan, the tasks below were assigned to National Research Institute of Electronics and Cryptology (UEKAE), a branch of Center of Research for Advanced Technologies of Informatics and Information Security (BİLGEM), an affiliate of Scientific and Technological Research Council of Turkey (TÜBİTAK);

1. Establishing a "computer emergency response team (CERT)" which will constantly track security threats in the cyberspace, publish notices, inform the public about how to take precautions against those threats, be able to coordinate counter measures in case of the realization of those threats,

2. Defining the minimum security levels necessary for government agencies, determining the security levels of the systems, software and networks used by the government agencies and presenting proposals about eliminating the deficiencies.

In this framework, Turkey Computer Emergency Response Team (TR-CERT) was founded under the structure of TUBİTAK BİLGEM UEKAE. The first National Information Systems Security Exercise (CERT 2008 Exercise) was held with the participation of 8 government agencies in 20-21 November 2008 under the studies of TR-CERT.

Then, in 5 November 2008, the Electronic Communications Act (ECA) numbered 5809, which made the following regulations regarding information security, was entered into force:

1. The principle of protecting information security and the privacy of communications should be taken into consideration by Information and Communication Technology Authority (BTK) within the regulations to be made.

2. BTK is assigned and authorized to take the precautions set forth by law in order to ensure national security, public order and smooth operation of public services for the electronic communications sector.

3. Protecting personal data and privacy and ensuring network security against unauthorized access are among the liabilities that BTK will bring

to the operators.

BTK conducts various activities on cyber security in virtue of not only the authorization given to it by the ECA numbered 5809, but also its being the ITU member representing Turkey.

Taking into account the legislative situation emerged after the enactment of the Electronic Communications Act numbered 5809; in 2010, BTK and TÜBİTAK BİLGEM UEKAE, cooperating with the objective of organizing a more comprehensive exercise with more participation than CERT 2008 Exercise, initiated the preparatory activities of the NCSE – 2011.

During the preparatory process of NCSE - 2011, it was observed that the concept of cyber security was brought to the agenda of the executive level bodies of the government and the National Security Council requested a presentation on cyber security from TÜBİTAK BİLGEM for the council meeting in October 27, 2010. In the so-called meeting, the Chairman of TÜBİTAK BİLGEM informed the council members via his presentation entitled "National Operating System and Cyber Security".

1.1. Objective

The main objective of NCSE - 2011 held in 25-28 January 2011 under the coordination of BTK and TÜBİTAK BİLGEM UEKAE is to make a significant contribution to the improvement of administrative, technical and legal cyber security capacity in Turkey, to enhance intra and inter organizational information and experience sharing and to raise awareness at every level, in particular the management level and to determine the organizational competence for computer emergency response.

By NCSE - 2011, it is also intended that the current situation, identified in the exercise by evaluating the responses of the participants against several cyber security violations, the capacity used for these responses and the inter organizational coordination, is to constitute input for future national and international studies on cyber security.

1.2. Scope

NCSE - 2011 was carried out in 25-28 January 2011 with the participation of 41 public, private and non-governmental organizations (NGOs) including judicial and law enforcement agencies and various ministries as well

as the ones from a diverse set of sectors such as finance, information technology and communication (ICT), education, defense and health. (See Figure 1). Six of those organizations participated in the exercise as observers. Approximately 200 officers who are experts in the fields of ICT, law and public relations from the participatory organizations attended the exercise. In NSCE – 2011, not only the technical competence but also the intra and inter organizational coordination capabilities of the participants were evaluated by measuring their responses to the cyber attacks in both the real and the simulation environment.

The profile of the participatory organizations according to their sectors is in Figure 2, the profile of their representatives according to their expertises is in Figure 3. The list of the participants is presented in Appendix-1.

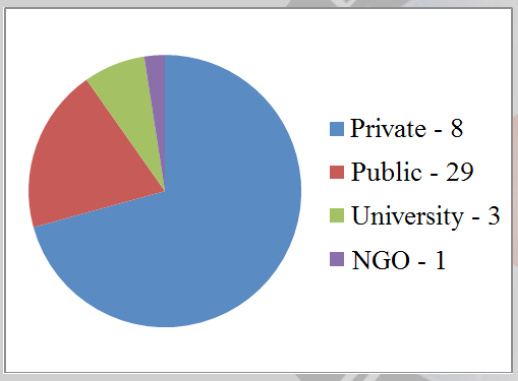

Figure 2. The Profile of the Participatory Organizations according to Sector

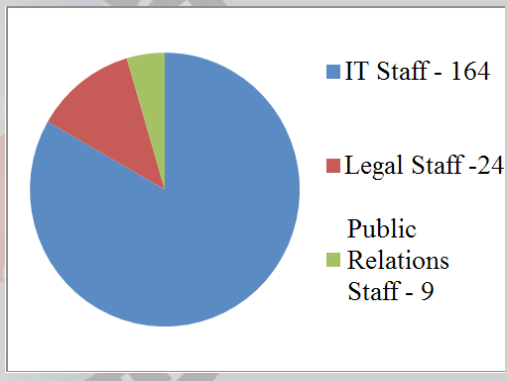

Figure 3. The Profile of the Representatives according to Expertise

As seen in Figure 1 in the Executive Summary, it was paid attention to the fact that most of the critical sectors, defined as the sectors that should be primarily protected in most of the developed and developing countries, in particular in the European Union (EU) and United States of America, provided participation in NCSE - 2011. When compared to the participants of CERT-2008 held in 20-21 November 2008, it can be more clearly noticed that NCSE - 2011 is more comprehensive. On the other hand, studies will be made for including the other critical sectors such as energy, food and agriculture to join in the cyber security exercises planned to be held in the future.

1.3. Targets

During NCSE - 2011, it was targeted to be on the alert against the cyber threats becoming more concrete day by day, to determine the computer emergency response capability and the inter organizational coordination of the participants, to improve communication and information and experience sharing among organizations and to raise awareness of cyber security. Necessary steps were taken in this direction.

1.4. Planning Process

The preparatory studies for NCSE - 2011 carried out under the coordination of BTK and TÜBİTAK BİLGEM UEKAE within the framework of 2006-2010 Information Society Strategy and Annexed Action Plan and the ECA numbered 5809 were initiated in February 2010 as a result of correspondences between BTK and TÜBİTAK. The planning process lasted approximately one year. During this process, the parties to participate in the exercise were invited, the relevant parties exchanged their views, and the studies for the logistic needs were conducted after determining the place of the exercise. The real attacks and the written injections to be carried out in the exercise were also planned in parallel to those studies.

The Preparatory Meetings

The preparatory meetings with the participants constituted one of the most important stages in the planning process of the exercise. In these meetings, not only the participants were informed, but also the parties exchanged views, so the process was shaped.

Almost 60 officials from 23 different public and private organizations attended to the first preparatory meeting at 29 April 2010. The participants were informed about both the exercise held in 2008 and NCSE - 2011 in the meeting, and their ideas about the issue were exchanged. At the end of the meeting, the parties were requested to declare their intention about participating in NCSE - 2011.

The second meeting was organized with the voluntary participants of NCSE - 2011 in 13 July 2010. In that meeting, the scenarios to be implemented were discussed and the participants were requested to contribute to the injections to be made during the exercise.

After the first two meetings, the public and private organizations to participate in NCSE 2011 were determined in a voluntary basis and they were informed about the general structure of the exercise. Then, the participants were categorized according to their sectors as the;

- Judicial and Law Enforcement Agencies,
- Finance sector,
- Universities,
- Telecommunication sector (including the ISPs),
- Defense sector,
- Other ministries

Then, several meetings entitled "focus group meetings" were carried out with each sectoral group in order to improve special injection for each sector and to closely learn about each sectors' own information systems. In total, 10 focus group meetings were made in August-September 2010.

The last preparatory meetings before the exercise were held in three groups in 11-13 January 2011. In those meetings, the participants were informed about the special messaging platform to be used in the exercise, wireless network infrastructure, and they were explained about the written injections and what kinds of responses were expected.

1.5. Scenarios

In the first two days of NCSE - 2011 carried out in 25-28 January 2011, the participants joined in the exercise from their own premises. The last two days of NCSE - 2011 were collectively fulfilled at the Conference Hall of TOBB Economy and Technology University.

Both the real attacks and the written scenarios were actualized in order to determine the technical competence of the participants, and to provide the participants with response experience in case of the possible attacks during NCSE – 2011, the second national cyber security exercise held in Turkey.

The number of the public and private organizations, to which the real attacks and the written scenarios were applied on a voluntary basis in NCSE

- 2011, is given in Figure 4.

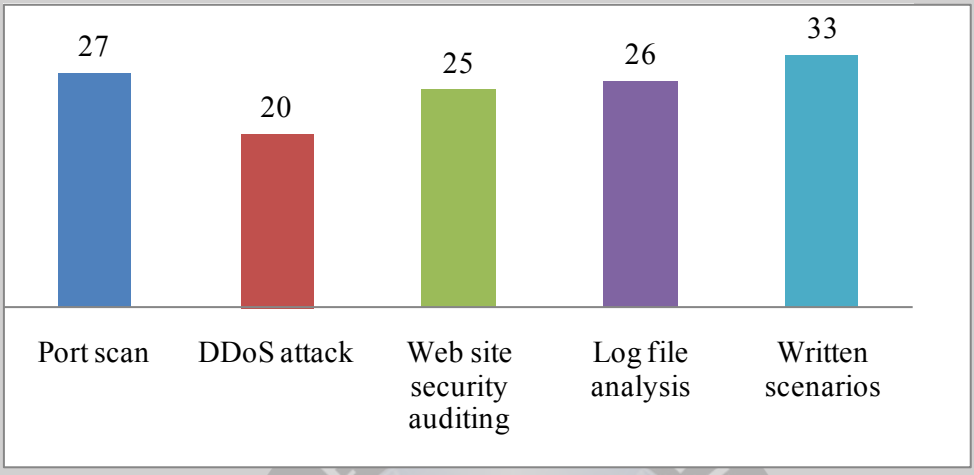

Figure 4. The Number of the Participants to which the Real Attacks and the Written Scenarios were Applied

1.5.1. Real Attacks

Within the context of the real attacks applied on a voluntary basis in the first two days of the exercise, four different activities were performed;

1. Port Scanning,
2. DDoS Attacks,
3. Website Security Control,
4. Log File Analysis

More detailed information on these activities as well as their findings is provided in part “2.Exercise Findings”.

1.5.2. Written Scenarios

At the collective session in the last two days of the exercise, 14 different written scenarios (injections) were sent to each of the participants in approximately one hour intervals and they were required to send their response they would give in case of facing these scenarios in real life in a written way to the exercise coordinators in one hour.

The content of the written scenarios sent to the participants were as follows:

1. Unauthorized manipulation of the content of the participant's official website

2. The detection of a DDoS attack from an IP address of the participant to another organization

3. The detection of spam message sending from an IP address of the participant to another organization

4. A DDoS attack to the participant from another source

5. The fact that a malicious insider who left the participant damaged the database before leaving

6. The infection of the participant's systems with a worm that was spread via the Internet

7. The attempt of stealing information from an employee of the participant by phone

8. The attempt of stealing information from an employee of the participant via e-mail

9. The detection of access of the employees of the participant to a site to which the access was prevented within the framework of Law No.5651

10. The detection of spam message sending from a fake website that looks as if it belongs to the participant

11. The breaking off the fiber line connecting the participant to the internet as a result of an unauthorized excavation

12. The breakdown of the cooling system in the system control room of the participant outside working hours

13. The fact that the generator system was not activated despite the power cut in the region of the participant

14. The detection of a wireless access point in the participant's premi-

se that can be easily connected by estimating its name

In this part of the exercise, the following issues were evaluated by assessing the responses of the participants to the above written scenarios:

- What kind of precautions they took within the organization,
- How they enabled coordination between their units,
- What kind of studies they carried out in order not to reflect the event outside the organization,
- Whether they contacted with the judicial authorities when necessary or not.

1.6. Other Issues

Security and Confidentiality

Utmost attention was paid so that no information about the participants and the exercise was let out before and after the exercise. Third parties were prevented to get information about the participants' systems and the vulnerabilities determined via the real attacks. The special reports prepared for each participant after applying web application control were shared with only the relevant organization.

Several preventive measures were taken against possible attacks to be targeted at the participants and the organizers of the exercise. Also, alternative communication methods were determined in order to overcome the prevention of the implementation of the exercise by potential problems. Appropriate security measures were taken in the last two days of the exercise when the written injections were actualized.

Public Relations

Several studies were made to have NCSE - 2011 known by the public. While raising awareness via publishing articles in the sector journals, also the relevant notices were published on the websites of BTK and TÜBİTAK. The exercise had become the focus of great interest from the press, national television channels and newspapers gave place to the related news.

The official opening ceremony of the exercise took place in 27 January

2011 with the participation of State Minister and Deputy Prime Minister Mr. Bülent ARINÇ, State Minister Mr.Prof.Dr. Mehmet AYDIN, Minister of Transportation Mr. Binali YILDIRIM, The President of BTK Mr.Dr. Tayfun ACARER, The President of TÜBİTAK Mrs.Prof.Dr. Nüket YETİŞ and authorized experts from BTK and TÜBİTAK BİLGEM.

2. FINDINGS OF EXERCISE

In this part, the findings determined as a result of evaluation of the responses of the participants to the real attacks and the written scenarios applied in NCSE - 2011, as well as recommendations for dealing with them are provided.

Finding 1. Lack of ISMSs:

It was detected that some of the participants did not have an ISMS established, any written policies, especially information security policy, procedures and instructions prepared or any risk analysis done. It was also observed that the participants did not have an information security culture with regard to dealing with information security vulnerabilities, and how to determine the corrective and preventive actions in order not to face any cases similar to the ones in the exercise.

Explanation:

ISMSs provide organizations to manage security violation cases from the beginning to the end and to take precautions not to experience that kind of cases again. Thanks to the predetermined processes this kind of systems include, the activities are primarily planned, then implemented, controlled and at the last stage necessary corrective activities are performed to fix the deficiencies identified in the control stage. Via the continuous operation of this process, an ISMS is established in an organization. Within the content of an ISMS, the entities in the organizations, the vulnerabilities of and the threats that can be effective on those entities are listed; thus the organizational risk assessment is carried out. The risk assessment document constitutes as input for the process of determining the measures that should be taken.

Recommendations:

ISMSs should be established and the policies, procedures and the instructions should be stored in written by the participants. Inventories of information entities of the organizations should be made by taking into account their confidentiality, integrity and accessibility values. The threats that can affect the information entities of the organizations should be determined and their risk analysis should be made. At the end of the risk

analysis made, the measures to be taken should be defined and implemented. The organizations should be periodically audited and the necessary corrective and preventive actions to overcome the vulnerabilities and non-compliances determined by auditing should be fulfilled.

Finding 2. Technical Incompetency of System Administrators:

In some of the participatory organizations, it was determined that the system administrators did not have sufficient technical knowledge to deal with a problem in the system; therefore the problem-solving time was longer than it should be.

Explanation:

System administrators are primarily expected to have sufficient knowledge about an organization's systems they are responsible for. The first step to take to satisfy this need is to provide the system administrators with relevant trainings. Also, a consistent and effective approach should be applied in managing information security incidents. After solving an information security incident, the personal knowhow obtained by the system administrators should be turned into organizational knowhow.

Recommendations:

System administrators should receive necessary technical trainings about the systems they are responsible for. Also, in order to measure the efficacy of those trainings, system administrators should take the exams for receiving the internationally recognized certificates in that field. If there is only one system administrator in an organization, (s)he should have expertise in a diverse set of fields such as border security systems, database systems, operating systems or web applications. However, if this is the case, that single system administrator will be a critical staff in that organization. In order to avoid such a case, more than one system administrator can be appointed in the organizations. In this case, the system administrators can back up each other by taking the responsibility of certain critical issues. Besides the technical trainings, system administrators should also take information security trainings about the systems they are responsible for. In order to ensure that a consistent and effective approach is applied in managing information security incidents, after solving an information security incident, the personal knowhow obtained by the

system administrators should be turned into organizational knowhow by identifying policies and procedures to measure and monitor the kinds, existence frequencies and the financial damage of information security incidents.

Finding 3. Lack of Intrusion Detection Systems and Processes:

It was observed that IDSs were not used by some of the participants with the aim of taking precaution against the regular attacks. On the other hand, as to the participants having IDSs, it was noticed that the logs produced by those systems were not examined effectively; therefore difficulties were experienced in detecting the attacks.

Explanation:

IDSs provide organizations to examine the received data packages and store the records of attacks or information collection activities via identified signs. IDSs are located on two points, one in the front and one on the back of firewall, in small and medium-sized networks. As to the large networks, IDS sensors can be installed on any point considered as necessary, further on the servers considered as important.

IDSs are not plug and play devices like many security hardware and software. The efficient use of IDSs depends on configuring them according to security needs to be determined after the installation, and the regular examination of the records the produced by them.

Recommendations:

The organizations which do not have an IDS should definitely have one and locate the system considering the complexities of their networks. Also, the system administrators should attend trainings about these systems, if possible take the related exams and receive their certificates. The system administrators should configure the IDSs properly according to the security needs of the systems they are responsible for, the records these systems produce should be regularly examined and reported. As the efficacy of these systems cannot be tracked instantly in application, the policies and procedures providing the efficient use of them should be identified by producing daily, weekly and monthly reports.

Finding 4. Lack of Awareness about Social Engineering Attacks:

It was detected that some of the participants searched for only technical solutions to security events, and ignored the human factor, which is the most important link in security chain.

It was also observed that in some of the participants, the personnel were not provided with regular awareness training regarding social engineering attacks, and information security reminder methods like sending warning e-mails to the users regularly and hanging information security posters at certain places of the workplace were not used effectively in order to prevent this kind of attacks. In addition, it was noticed no periodic social engineering tests were conducted with the purpose of increasing resilience of the personnel against such attacks.

Explanation:

Social engineers benefit from people to obtain valuable information with or without using technology, and mostly use influence and persuasion methods. Social engineering can be described as the art of getting people do something which they normally do not do for unfamiliar people. This kind of threats can come from unexpected places at an unexpected time and can be from within or outside an organization. In case of a social engineering attack, erroneous information sharing arising from the weakness of a single personnel may cause wounds that would deeply affect the organization, financial and time loss, even loss of life and damage organizational reputation.

Recommendations:

The organizations should have their employees approach with caution against the requests from unfamiliar people and not share their personal information such as user passwords with anybody including system administrators, their colleagues and managers. All employees should be provided with information security awareness trainings periodically; and efficacy evaluations should be carried out at the end of those trainings. Also information security tests including social engineering attacks tests should be periodically performed in the organizations. Information security reminder methods like sending warning e-mails to the employees regularly and hanging information security brochures at certain places of the workplace

should be implemented.

Finding 5. Outdated Antivirus Systems:

It was determined that the signature files of central antivirus servers were not regularly updated; therefore the signature files of antivirus software, installed on end units and updated from the central antivirus servers, were not periodically updated, either.

Explanation:

A computer virus is a computer program which attempts to hide itself in the other files and changes the way the computer works without the user's knowledge or permission. A real virus has the capability of replicating and executing itself within the environment it infects. Antivirus software are developed and used in order to avoid this kind of malicious codes. It is an important point that the signature files, which the antivirus programs use while identifying viruses, are regularly updated in order to detect newly generated viruses.

Recommendations:

All client computers should be updated from a central antivirus server for the efficient use of antivirus software in the organizations; signature files should be kept up-to-date, automatic protection features should be activated on all computers and if possible, different antivirus software should be installed on different servers. For example, while installing antivirus software on file server, antivirus software developed by different producers should be installed on the e-mail server and end user computers because a malicious code that can be detected by an antivirus software may not be detected by another one. By this way, the capacity of detecting malicious codes within the organization's network can be increased.

Finding 6. Incompetency of System Administrators in terms of Security:

It was observed that the system administrators in some of the participatory organizations did not have necessary competence for information security; also the participants were not in contact with security interest groups, other specialist security forums and professional associations.

Explanation:

Information security has different properties such as accuracy, accountability, reliability and non-repudiation in addition to confidentiality, integrity and availability of information. The fact that information security activities are carried out in a department such as the "information security department" instead of the "information processing department" where the system administrators work for, constitutes as the framework of the main precautions that should be taken to effectively response to security violations.

Recommendations:

Information security units can be established in the organizations to effectively response to security violations. In this unit, apart from the system administrators, the employees who will be responsible for only information security can be charged. This staff should take trainings for technical issues such as border, database, operating systems and web applications security. In addition to these, they should be provided with trainings about the administrative aspects of information security such as the establishment and auditing of ISMSs and business continuity. This unit should also be in contact with special interest groups, other specialist security forums and professional associations.

Finding 7. Lack of Intra-Organizational Coordination:

It was detected that the coordination among the internal units in most of the participants was insufficient, some units were not provided with substitute staff. Therefore, in case of an information security event, the necessary steps could not be taken, and either no contact or late contact with the corresponding authorities could be made.

Explanation:

Intra-organizational critical units responsible for information technology, information security, legal affairs and public relations have to ensure the necessary coordination among each other in order to give fast and accurate responses in case of any security violation. Substitute staff should be provided for business continuity in the critical units for which only one officer is responsible. For timely response against information security vio-

lations, effective inter-organizational coordination is critically important.

Recommendations:

One of the most effective ways to ensure the necessary coordination among the critical units responsible for information technology, information security, legal affairs and public relations in order to give fast and accurate responses in case of security violations, is to arrange written and practical exercises in the organization periodically. Also, lists of contact information should be formed, regularly reviewed and updated and the related persons should be provided with easy access to these lists for contacting with the relevant authorities timely. Substitute staff should be employed for business continuity in the critical units.

Finding 8. Lack of Access Control Policies:

Some of the participants did not have an access control policy that uses business and security requirements as base for access. As a result of this, the staff could gain unauthorized access to irrelevant information and services.

Explanation:

Access control, in its simplest definition, is implemented to provide only the authorized person or groups with accessing a certain entity within the defined rights and within the defined period of time. This access can be both physical and logical. Logical access, in its most general form, defines the accesses to an information entity via computer.

Recommendations:

An access control policy using business and safety requirements as base for access should be formed; the policy should be documented and regularly reviewed. The access rights of all users should be determined and clearly pointed out in the policy document. The policy document should arrange the principles of physical access besides the logical access. While determining the access rights, the principle of “Everything is forbidden unless authorized”, which is stricter than the approach “Everything is free unless forbidden”, should be adopted. Requesting for access rights, giving consent to the requests and updating the rights in the information system should be fulfilled by different authorities. The removal of access rights

of the an employee who leave the organization or whose job is changed is one of the important components in access control. The active access rights in the information system should be regularly reviewed. Forming an Access Control Policy document that gives the definitions of all of these issues, and the comprehension and adoption of the document by the employees will provide to healthfully apply the access control, which is one of the most important components of information security within an organization.

Finding 9. Ignoring Security at the System Design Stage:

It was noticed that some participants had not consider security as a main design principle at the system design stage; which caused security breaches to occur and complicated effective response against the security cases.

Explanation:

While building a corporate information system, the system design process is composed of several stages such as the topology design, distribution of IP addresses, naming the computers, setting user accounts and ensuring scalability. The system design is important for detecting information system components that are affected by an information security incident, quarantining those components and isolating them from the corporate information system when necessary and determining the source of the attack timely. A system designed by taking information security principles into account is a more manageable system in the sense that response against information security incidents can be given in an easier and more effective way. However, things get more complicated in a system not designed so.

Recommendations:

In order to response against information security incidents in an effective way, the system operated, if possible, should be redesigned by considering security as a principle. If redesigning the system is not applicable in the short term, various arrangements can be extended over a period of time with proper planning. One of the most important stages in the system design process is system topology design. As it is difficult to change the system topology after the system is put into use, expert support can be

get at that stage. The distribution of IP addresses, setting user accounts, removing the duplicate accounts and the implementing the principle of segregation of duties can be assessed in this context.

Finding 10. Risks arising from Wireless Networks:

It was observed that some of the participants could not detect the unauthorized wireless access points installed by the attackers; from which the personnel might get service.

Explanation:

Wireless networks are network structures enabling the connection of the devices, capable of wireless communication (802.11, Bluetooth, IR (infrared), GSM etc.), to each other without a physical link. The risks of wireless networks are wired network penetration, data resolution by listening to the network traffic, elicitation of the network topology, the connection of clients to the unauthorized access points, denial of service and serving to the unwanted clients.

Recommendations:

According to the results of risk analysis, a real-time IDS, which constantly follows the environment in which wireless access is available, alerts in case of familiar kinds of attacks and detects the unauthorized access points and the clients, can be used in the organization. The users should be informed about the security measures and be prevented to accidentally deactivate those measures. The wired network should not be connected via Ethernet interface on any user computer during wireless connection. Otherwise, that user computer can function as a bridge between the wireless network and the wired network. Also, access points and wireless bridge devices should be located properly so that they are safe against stealing or intervention.

Finding 11. Lack of Business Continuity Plans:

It was detected that some of the participants did not have a business continuity plan established for preventing business interruption and maintaining business processes in case of an information security incident causing system interruption.

Explanation:

Business continuity consists of the studies to maintain the critical business processes of an organization; and if maintenance is not possible, to make the business processes functional again within a predetermined maximum acceptable interruption time. Theoretically, it is expected that the critical business processes are always on. However, interruption is inevitable because of certain incidents. Some of those incidents can be small and recovered in the short term, while the others can be serious disasters.

Recommendations:

Business continuity studies should be performed in the organizations in order to be affected by possible business interruptions at the minimum level. In this context, business impact analysis, which primarily includes the critical business processes and the maximum acceptable interruption time for each process, should be made. After business impact analysis, incident management plans and business continuity plans should be formed in a strategical sense. These plans should be periodically tested by exercises. After then, a contact list to which all relevant employees can access should be created. The other steps to take are establishing substitute systems, installing automatic alert systems independent of staff, coordinating the relations of the parties within the framework of business continuity and founding a disaster recovery center if needed as a result of the analysis.

Finding 12. Inability to Detect Port Scan Attacks:

It was noticed that some of the participants could not detect "Port Scan" attacks against their information systems connected to Internet.

Explanation:

Port scan, one of the first actions the attackers make before beginning an attack, aims to detect open ports and discover the vulnerabilities on the targeted system. Ports can be defined as the doors that connect the user computers to the outside world. Port scan neither damages the systems nor puts the confidentiality of processed information at risk. The competency of the participants to detect a scan from outside to their systems was observed via port scans carried out during NCSE - 2011.

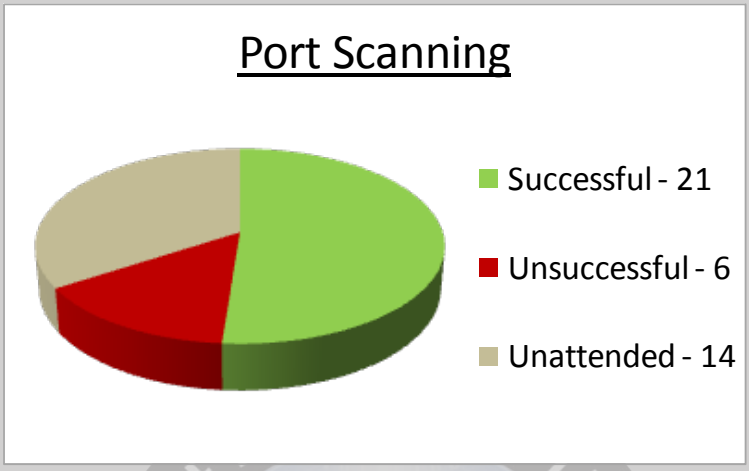

Figure 5. The Results of Port Scan Attack

In NCSE - 2011, 27 of the participant organizations volunteered for the performance of this attack against their systems during the exercise and expressed that they had the necessary systems to detect this attack in the preparatory meetings before the exercise. At the result of the attack, although 21 participants could successfully detect the attack, 6 participants could not detect it (Figure 5).

Recommendations:

Configuration of Firewall, IDS and the similar border protection systems prepares the technological infrastructure for an organization to detect "Port Scan" attacks. In addition to this infrastructure, there should be system administrators responsible for regularly observing the logs, alerts and similar data produced by the systems.

Finding 13. Unfavorable Results of DDoS Attacks:

It was detected that as a result of DDoS attacks, most of the participants experienced a business interruption; the ones that did not have business interruption were the ones that purchased service from their Internet Service Providers (ISS) in order to be protected from this kind of attacks. This reveals the importance of inter-organizational communication, cooperation and coordination for enabling information security.

Explanation:

Today, DDoS attacks take one of the first places among the attacks for preventing the systems' operation. In these attacks, the users who normally can access to the system are prevented to connect it via intensively sending packets (network traffic) from different sources to the targeted system, DDoS attacks were performed at certain times within the framework of NCSE - 2011 in order to determine how durable the participants' systems were to this kind of attacks and to improve their capability of response to possible similar attacks.

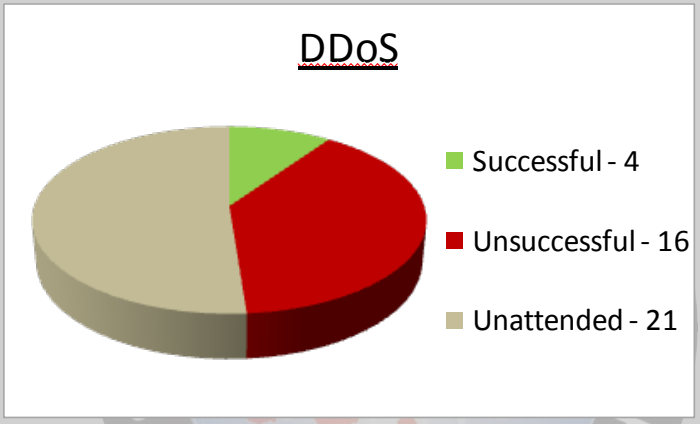

Figure 6. The Results of DDoS Attacks

For each of the 20 of the participants that were voluntary for this attack, a DDoS attack was carried out for a period of previously reported 2 hours outside the working hours. While 16 of the participants had business interruption during the attack, 4 of the participants were able to survive (Figure 6). It was observed that the participants that did not have business interruption were the ones that purchased special service from their ISPs in order to be protected from this kind of attacks. This reveals the importance of inter organizational communication, cooperation and coordination for providing information security.

Recommendations:

Although there is no exact solution to eliminate DDoS attacks, taking the precautions below can bring positive results:

- Using open source operating systems in server devices providing

service, taking measures like “SynCookie” on these operating systems.

- Continuously using border monitoring systems, which are on the network of the server which is attacked, and when an attack starts, determining the common features of the packets in the attack and filtering out these packets by the systems like firewalls etc.

- Application of necessary policies to filter out the attack packets at the starting points of the networks for which each ISP is responsible for across the country.

The IT staff should have knowledge about current attack kinds like DDoS to be able to apply precautions similar to the above and they should be trained about these issues. By this way, they can detect an attack against their organization timely and correctively, work for preventing the attack and contact with the relevant organizations. The participants can purchase service for preventing DDoS attacks from their ISPs. During this kind of attacks, necessary and sufficient coordination should be ensured with ISPs. The agreements, signed between the organizations about the quality and level of the services ISP will provide should be reviewed, necessary contacts from ISP in case of an incident should be clearly defined. The functionality of them should be checked before an attack case.

Finding 14. Vulnerabilities in the Web Applications:

Certain vulnerabilities were detected in the web applications running on the participants’ information systems connected to Internet. The participants considering security as an essential requirement during application development and having their applications checked by independent government agencies and organizations were noticed to have respectively less vulnerabilities in their web applications.

Explanation:

The web sites of the organizations are especially the target of the attackers wishing to damage the organizational reputation. In the attacks made against Estonia and Georgia in 2007 and 2008, which are noticed as examples of the first cyber wars in the World, it was remarkable that the most common attack methods were attacking and changing the content of government web sites. In NCSE - 2011, the security of the participants’ web sites was controlled according to the perspective of an attacker.

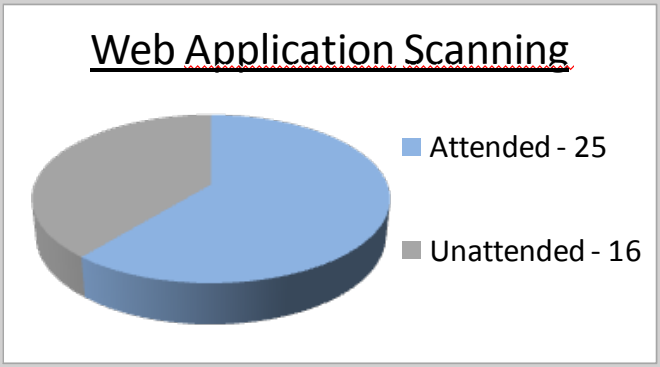

Figure 7. Participation in Web Applications Analysis Study

In NCSE - 2011, 25 participants volunteered for this attack (Figure 7). Totally 66 applications declared by those participants were checked. The graphic classifying the detected vulnerabilities as High, Medium and Low according to their levels of importance is presented in Figure 8. The names of the participants are expressed as numbers for the sake of confidentiality. A special report was prepared for each of the participants that vo-

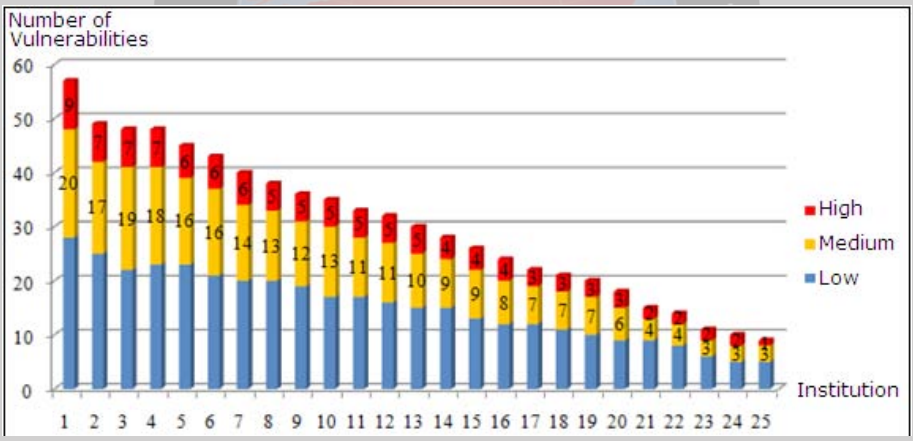

Figure 8. Numbers of the Web Vulnerabilities detected in the Participants

lunteered for web application control and was submitted to the relevant organization. The participants, considering security as a basic need during application development and having their applications checked by the independent agencies, were noticed to have respectively less vulnerabilities in their web applications.

Recommendations:

As expressed at the end of the explanation part, “secure software development” practices should be put into effect at the stages of web application design and implementation. The practices can be implemented by either the organization itself or the third party software developers. In either case, a business process including both administrative and technical aspects should be carried out. Independently testing the developed software is an extremely important need; and how to meet this need should be defined within the context of the software development process.

Finding 15. Inability to Analyze the Log Files Properly:

Some of the participants were observed not to be able to determine when, how and by whom the attack was carried out by means of analyzing the attack log files formed during the attacks made within the context of the exercise. The participants which had a special information security unit were observed to be respectively more successful.

Explanation:

Analyzing the log files generated during an attack enables to detect when, how and by whom the attack was carried out. Various attack logs formed via the attacks produced in the test environment were sent to the participants during NCSE - 2011 and the participants were required to detect when, how and by whom the attack was carried out.

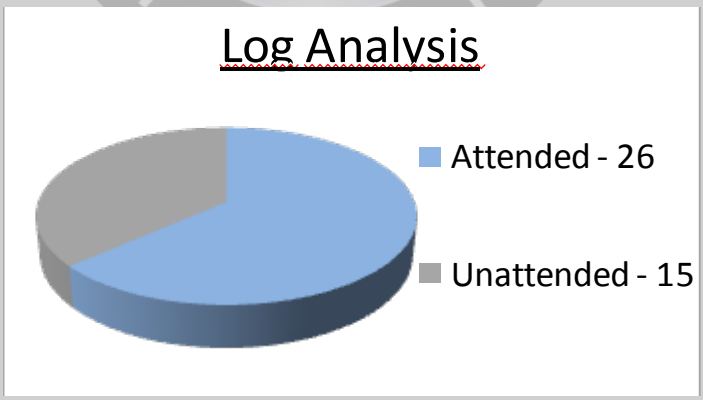

Figure 9. Participation in Log File Analysis

It was aimed to both provide the participants with log analysis experience and observe their current competence on that issue in NCSE - 2011. 26 participants volunteered for log file analysis (Figure 9). 5 different log files that were compatible with the participants' operating systems (Linux, Windows, etc.) were prepared for and several questions were asked to each one of these participants. The participants which had a special information security department were observed to be respectively more successful.

Recommendations:

The solutions were practically discussed in a workshop arranged after the exercise in order to achieve the aim of providing the participants with experience on log file analysis.

3. RESULT AND RECOMMENDATIONS

NCSE – 2011 was successfully completed in 25-28 January with the participation of 41 organizations after a preparatory process lasting approximately one year. In addition to over 500 written injections, the real attacks composed of port scanning, DDoS attacks, web application control and log file analysis were carried out in NCSE – 2011.

Findings and the General Situation

The findings reveal that the organizations participated in the exercise had a considerable amount of information security vulnerabilities.

It should be pointed out that purchasing hardware-software and making large amounts of investments to information technology are not enough to overcome the mentioned deficiencies. Instead; primarily the executives and all employees should be trained about information security, and additionally the organizational business processes related to information security should be put into practice.

Evaluating the findings generally, it is seen that studies should be made in the fields of ISMSs, business continuity, human resources, intra and inter organizational coordination; and also the efficiency of ongoing researches should be increased in order to enhance cyber security in Turkey.

ISMS for a Corporate Approach to Information Security

ISMSs have an important place among the activities done for providing corporate cyber security, which reduce the dependency of organizational security on the personal knowledge and capabilities of the employees and give the insight of measurement, monitoring and constant improvement to the organization. In NCSE - 2011, it was observed that the participants that had ISMSs made a more systematic effort to solve the problems at the stage of responding to information security incidents in the written scenarios.

Business Continuity

Studies for business continuity are critical for the preventing business interruption and providing the systems to run in a short time in case of any interruption. Therefore, organizations should primarily form business

continuity plans according to the analysis to be made. It was observed that the participants that had previously worked on business continuity could struggle with business interruptions more effectively and run their systems in a shorter time than the others as a response to the written scenarios carried out in NCSE - 2011.

Human Resources

The human resources is another crucial issue to take into account in the studies for providing cyber security. In this context, firstly, substitute staff should be employed, trainings for the system administrators to have a good knowledge about the system they operate should be planned and then information security expertise trainings should be planned for the expert staff who will work for information security (if possible, as a separate unit). Cyber security should not only be seen as a technical issue, but also should include studies to improve awareness and capacities of human resources of the organizations

Inter and Intra-Organizational Coordination

Finally, it is not possible for the organizations or their information processing units to response or produce solutions alone for the information security incidents. In order to be able to struggle with cyber security threats, the communication with both internal (information processing unit, legal unit, public relations unit and etc) and external partners should be improved and necessary coordination should be enabled.

APPENDIX 1: PARTICIPANTS OF NCSE - 2011

Public	Private	University	NGO
Ministry of Justice	Avea	Ankara University	Association of Information Security
Public Prosecutor of Ankara	Microsoft Turkey	ODTÜ	
Banking Regulation and Supervision Agency	TTNET	TOBB ETÜ	
Prime Ministry	Turkcell		
BTK	Türksat		
Undersecretariat of the State Planning Organization	Türk Telekom		
Undersecretariat of Foreign Trade	Vakıfbank		
Ministry of Foreign Affairs	Vodafone		
General Directorate of Security			
Turkish General Staff			
Undersecretariat of Treasury			
Ministry of Internal Affairs			
General Directorate of Finance Public Accounts			
Central Bank			
General Secretariat of National Security Council			
Ministry of National Defense			
General Directorate of Population and Citizenship Affairs			
General Directorate of Post, Telegraph			
Undersecretariat of Defense Industries			
Court of Accounts			
Capital Markets Board			
Social Security Institution			
General Directorate of Land Registry and Cadastre			
TÜBİTAK BİLGEM (PCC)			
TÜBİTAK BİLGEM Pardus			
TÜBİTAK BİLGEM UEKAE			
TÜBİTAK ULAKBİM			
Ministry of Transportation			

APPENDIX 2: PHOTOS FROM NCSE – 2011


Prof.Dr.
Mehmet AYDIN


DEVLET PLANLAMA
TEŞKİLATI


USGT


ULUSAL SİBER GÜVENLİK TATBİKATI
USGT
2011
ANKARA ÜNİVERSİTESİ


ANKARA CUMHURİYET
BAŞSAVCILIĞI


ATAVİZYON

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

TÜBİTAK