9 Methods and Means for Protection of Software Critical Infrastructures

9.1 Definitions

9.1.1 Infrastructures

According to "Etymology online" [Dictionary, 2010] a definition for the global infrastructure exists since 1927 and means: "The installations that form the basis for any operation or system". Originally, the term was used by the military.

Usually the term "infrastructure" refers to the technical structures that serve citizens. These are roads, water supply, sewage system, electrical network management systems in a flood, communications (internet, telephone lines, radio, and television), etc. In the past, these systems were usually owned and managed by local and central government authorities. These elements can be summarized as civil infrastructure, municipal infrastructure, or simply referred to as public facilities, although they can operate and develop in both the private sector and in state enterprises.

9.1.2 Critical Infrastructure

Infrastructure may refer to information technologies, formal and informal channels of communication, tools for creating software, political and social networks, or beliefs of certain groups of population.

The term "Critical Infrastructure" is used for those elements of infrastructure that if damaged severely or destroyed, would cause serious disruption of the depended system or organization. Storm, flood, or earthquake leads to the loss of key transport routes in the cities (e.g. bridges). This can prevent people to evacuate or rescue teams to do their work; these roads can be referred to Critical Infrastructure. Similarly, online registration systems can be Critical Infrastructure for airlines.

The notion of infrastructure lies not only on the public sphere and its facilities, but also on the working methods, management practices and policy developments in the direction of interaction between them all on the one hand, on the other – taking into account with the social needs and assuagement of public transport communications (for people and goods), providing drinking water and industrial water, safe waste disposal, energy supply and the need for dissemination of information among the population [21st Century, 1987].

IT infrastructure is an integral part of Critical Infrastructures and to achieve an effective protection of these Critical Infrastructures should primarily ensure the protection of Critical Information Infrastructures from malicious acts caused intentionally or unintentionally.

9.1.3 Software Critical Infrastructure

Once explained what we mean by Critical Information Infrastructure for the purposes of this part of the book, we can define the following working definition of Software Critical Infrastructure. As Software Critical Infrastructure will note a set of specific software solutions designed to operate and manage the relevant Critical Information Infrastructures.

In most cases, when talking about infrastructure security is understood security of Critical Infrastructures such as airports, railway highways, hospitals, bridges, network communications, media, power grid, dams, nuclear reactors, seaports, oil refineries and water systems.

Below when talking about the protection of Software Critical Infrastructure will mind the following points:

- protection during the design of the software solution;
- protection during the build of the software solution;
- protection during the test of the software solution;
- protection during the execution of the software solution;

To protect critical software infrastructure must be taken into account following:

- to analyze and identify threats;
- to reduce vulnerabilities in Software Critical Infrastructure;
- to reduce to a minimum the amount of possible injuries;
- to minimize to a minimum the time for reaction while trying to attack, and the time of response reaction and recovery of the caused damages;
- to analyze the causes of damages and the attack source (human action, incorrectly written source code, etc.);

9.2 The current situation

Nowadays information society requires the use of various types of information flows. These information flows are usually in the form of file objects. On various types of file objects, the following main operations are applied: creating, processing, transferring / accepting and saving / storage [Dale and Lewis, 2009], [Cohen and Kalbaugh, 2008] (Figure 151).

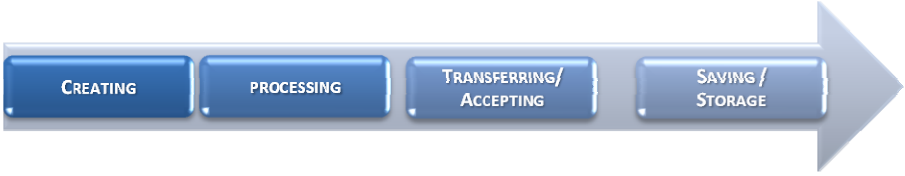

Figure 151. Main operations applied on file objects

In the process of creating of the object are generated its main parameters: filename, file format, header information, etc. This process is necessary to enable the opportunity of the object to be processed later, which includes some of the following operations related to the information included in the file: read, edit, copy, move, delete. Operation transferring / accepting of the file object is related to the possibility of the object to be sent to another device that is most often done by placing it on appropriate media or through the Internet, Extranet, or Intranet. Upon accepting of the object, it can be stored on local hard drive then its further processing could be possible.

During the investigation of the information security of objects, we should take into consideration they could be exposed to different information attacks. The information attacks can be provisionally divided into malware and malattacks (Figure 152).

In case of **malware** the direct participation of a user at the moment of the attack is missing, while in case of **malattack** the user's presence is required [Shaw, 2006], [Radhamani and Rao, 2007].

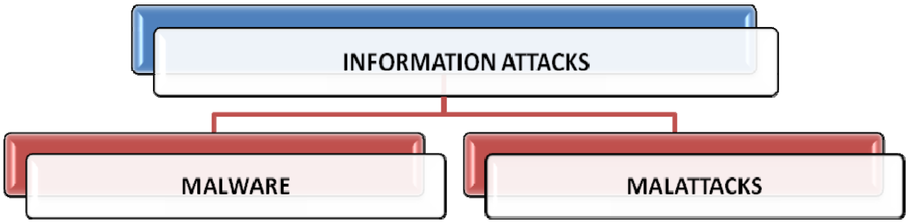

Figure 152. Main categories information attacks

The objects used in Software Critical Infrastructures exposed to attacks, may be possible in following states:

1) in cases where they are in an environment with method of protection (Figure 153);

2) in cases where they are in an environment without method of protection (Figure 154).

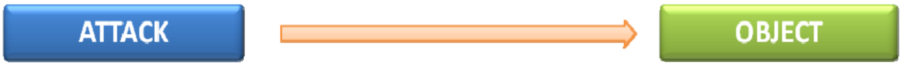

Figure 153. An object in environment without method of protection

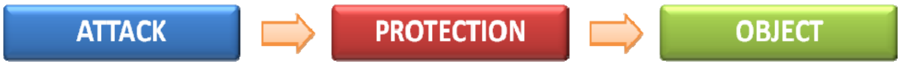

Figure 154. An object in environment with method of protection

When methods of protection of object from information attacks are investigated, they can be divided into three main categories: methods of protection depending on the environment, methods of protection depending on the architecture and method of protection depending on CPU characteristics (Figure 155).

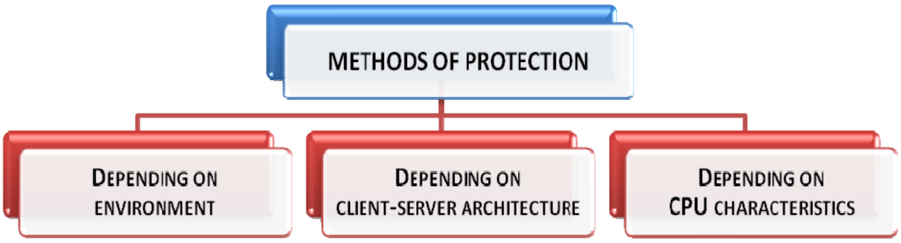
METHODS OF PROTECTION
DEPENDING ON ENVIRONMENT
DEPENDING ON CLIENT-SERVER ARCHITECTURE
DEPENDING ON CPU CHARACTERISTICS

Figure 155. Main categories methods of protection

9.2.1 Information attacks groups

A description of the groups of attacks, referred to the categories "malware" and "malattack" is given below.

In category **malware**:

(I). Browser related attacks [Dingledine and Golle, 2009], [Camenisch, 2009], [Dubrawsky, 2009]. These attacks are characterized by the fact that they use the resources and capabilities of different browsers in order to fulfill its malicious content. The consequences of such an attack can be insignificant (such as crashing of the browser), but they can lead to theft of identity or other confidential information.

(II). Metadata [Clarke, 2009]. The attacks from this group use the possibility to add metadata to file object to achieve their malware goal.

(III). Cracking [Sarknas, 2006]. The attacks from this group succeed to neutralize procedures of authentication, check sums, registration, etc.

(IV). Spying [Ciampa, 2008], [Ciampa, 2009]. The attacks from this group use means for illegitimate gathering information. Absolutely everything in the attacked system is subject to espionage.

(V). DoS, DDoS [Docter et al, 2009]. The goal of the attacks from this group is to make computer resources unavailable to its intended users.

(VI). Exploits [Rabe, 2009]. They use a security hole. It is used as the base to create programs that search vulnerable systems and those who enter the already found vulnerable systems;

(VII). Scanners [Erjavec, 2009]. The attacks from this group use different tools and techniques to scan the system. In most cases, they precede other malicious components.

(VIII). Keyboard modifiers [Newman, 2009], [Dubrawsky, 2009].The attacks from this group use techniques to spy and manage the keyboard, mouse and screen activity.

(IX). Computer Trojan Horses [Kartalopoulos, 2009]. It transports program components that are later used for some malignant goal. The term is often used to describe the malignant software that is transported.

(X). Computer Backdoors [Newman, 2009]. They create security hole as supporting a communication port in opened state.

(XI). Computer Worms [Ao and Gelman, 2009]. An independent program that spreads data from one computer to the next using the network connections and frequently takes advantage of the weakness of the main Internet protocols in order to cause problems in computer systems and networks. It is usually combined with spy and advertisement components.

(XII). Computer Viruses [Esl, 2009]. A parasite program that without the user's knowledge or permission attaches to the infected object procreates and continues to spread. It usually has a malignant component aimed at harming the functionality of single programs or the whole computer system. This term includes currently 50+ functional types.

In category **malattack**:

(XIII). Using accessible information [Blyth, 2006]. The attack possibilities are based on a previous illegitimate acquisition of logs, registers, documents, etc., that reveal the functioning and security of a given system. The specific information needed for the next attack can be found by studying the volume and the internal structure of the incoming and outgoing traffic in a computer system or network.

(XIV). Overflow. Hackers cause an overflow of certain buffers in order to have a system or network dysfunction or to receive or execute malignant code.

(XV). Vulnerabilities [FTC, 2010]. Usually the actions of the attackers are based on a serious security breach in the system. The administration of a certain application or group of applications is taken over.

(XVI). Content [Osborne, 2006]. A large variety of techniques based on destructive office macros, executable trojans and ActiveX, and Java applications.

(XVII). Data Encapsulation [Wrembel and Koncilia, 2007]. Data is hidden or capsulated in such a way that it overcomes the firewall and is then free to unite or fulfill its malignant mission.

(XVIII). Denial of Service [Sisalem et al, 2009]. The main goal of these attacks is to receive denial of service due to planned and coordinated service requests. The important in this case is the large number of hosts that make the requests, which causes exponential increase in the number of requests.

(XIX). Spoofing [Haldar and Aravind, 2009]. To attacks by this group can be summarized that their aim is to successfully masquerade by falsifying data and thereby gaining an illegitimate advantage.

(XX). CrackPasswd [Miller and Gregory, 2009], [Chandra et al, 2009]. This attack is relatively rare due to the current password-based site protection system. Some serious preparation is needed to access the passwords. Should that happen the attack could last relatively long because people are used to being safe.

(XXI). Zombie Computers [Wang, 2009]. Completely controlled by a hacker's computer. In this case, the attacker can create for example two super-zombies that on their own control, 8 other zombies and so on. In this manner, a large number of computers simultaneously attack a computer until they achieve denial of service.

Note: Roman numbers in brackets are used later as identifiers of the names of the attacks groups.

9.2.2 Objects groups

The groups of the objects can be referred to the categories "directly executable" and "indirectly executable". Directly executable objects can be directly usable, while indirectly executable objects require secondary processing to become directly usable.

Table 9 shows the groups of directly executable and indirectly executable objects that are most often subject to information attacks in Software Critical Infrastructure.

Table 9. Groups of objects that are most often subject to information attacks

Object group	Total [%]	Malware [%]	Malattack [%]
DIRECTLY EXECUTABLE			
Archived and Compressed	11,11	9,54	1,57
Scientific	10,86	9,22	1,64
Data	17,49	14,58	2,91
Internet related	16,00	13,50	2,50
Binary	17,53	14,81	2,72
Virtual machine	9,34	7,70	1,64
Other	5,94	4,88	1,06
TOTAL DIRECLTY EXECUTABLE:	**88,27**	**74,23**	**14,04**
INDIRECTLY EXECUTABLE			
Graphic	6,17	5,15	1,02
Audio and music	2,31	1,94	0,37
Video	3,25	2,72	0,53
TOTAL INDIRECTLY EXECUTABLE:	**11,73**	**9,81**	**1,92**
ALL OBJECTS	**100,00**	**84,04**	**15,96**

9.2.3 Protection groups

Figure 156 shows the protection’s groups used to protect file objects from information attacks in Software Critical Infrastructure.

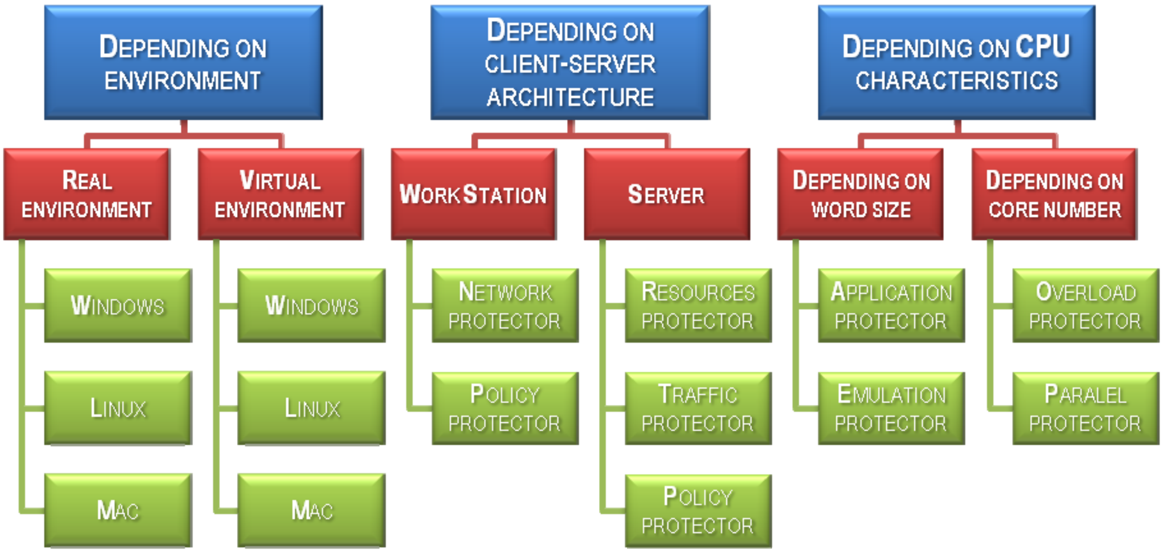

Figure 156. Main protection’s groups

I. Protection types depending on environment:

1) in case of real environment. It is protected by:

- real-time memory protectors;
- real-time registry protectors;
- real-time media (disk, CD/DVD, flash, etc.) protectors;

The most commonly used operating systems in a real environment and their protection types are:

1.1) Windows real environment. The protectors include:

- real-time Windows memory protectors;
- real-time Windows registry protectors;
- real-time Windows media (disk, CD/DVD, flash, etc.) protectors;

1.2) Linux real environment. The protectors include:

- real-time Linux memory protectors;
- real-time Linux registry protectors;
- real-time Linux media (disk, CD/DVD, flash, etc.) protectors;

1.3) Mac real environment. The protectors include:

- real-time Mac memory protectors;
- real-time Mac registry protectors;
- real-time Mac media (disk, CD/DVD, flash, etc.) protectors;

2) in case of virtual environment. It is protected by:

- virtual memory protectors;
- virtual registry protectors;
- virtual media (disk, CD/DVD, flash, etc.) protectors;

The most commonly used operating systems in a virtual environment and their protection types are:

2.1) Windows virtual environment. The protectors include:

- virtual Windows memory protectors;
- virtual Windows registry protectors;
- virtual Windows media (disk, CD/DVD, flash, etc.) protectors;

2.2) Linux virtual environment. The protectors include:

- virtual Linux memory protectors;
- virtual Linux registry protectors;
- virtual Linux media (disk, CD/DVD, flash, etc.) protectors;

2.3) Mac virtual environment. The protectors include:

- virtual Mac memory protectors;
- virtual Mac registry protectors;
- virtual Mac media (disk, CD/DVD, flash, etc.) protectors;

II. Protection types depending on client—server architecture:

1) on behalf of Workstation the following protections can be referred:

1.1) Network protector. These type protections analyze the TCP/IP packets and recognize malware content;

1.2) Policy protector. A user profile, threat assessment and security policy choice is made;

2) on behalf of Server the following protections can be referred:

2.1) Resources protector. They protect single shared resources (memory, disk, periphery);

2.2) Traffic protector. Protection aims to prevent unusual, abnormal traffic;

2.3) Policy protector. A Work Station's profile is created, a malware content is recognized and correct security policy is chosen for each Work Station.

III. Protection types depending on CPU characteristics:

1) depending on word size the following protectors can be observed:

1.1) Application protector. They must be conformable to the application's word size as taking into account the relationship between the operating system and the word size;

1.2) Emulator protectors. These protections include defense against unwanted or incorrectly selected emulations of processes, applications, and resources.

2) depending on core's number the following protectors can be observed:

2.1) Overload protector. They include protection against overloading of dataflow with respect to one or more cores;

2.2) Parallel protectors. They include protection against malicious or accidental breach of parallel processing of the information by the single cores.

9.3 Available information for accomplished attacks

An analysis will be presented here, based on the current information base of National Laboratory of Computer Virology of Bulgarian Academic of Sciences. It collects information for the information attacks, which were carried out to a separate personal and/or corporate computers, and/or networks, and/or systems for 2009. This is a generalization of attacks, implemented in Bulgaria, Balkan Peninsula, and southeast Europe. Figure 157 shows the percentage distribution of accomplished attacks' groups. Summary, 84% from them belong to the **malware** category, and 16% belong to the **malattack** category.

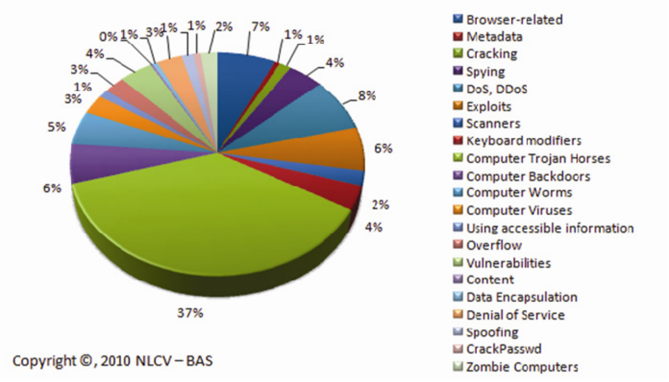

Figure 157. Percentage distribution of accomplished attacks' groups

Compared with the other structures (government, corporate and users), the number of accomplished attacks to Critical Infrastructures as a hole is about 23% (Figure 158).

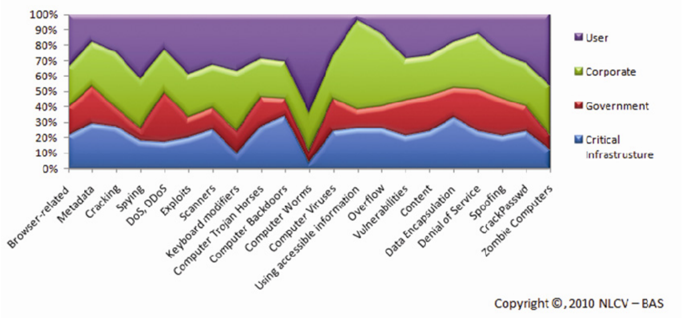

Figure 158. Percentage distribution of attacks' groups, accomplished to computers, systems and networks with respect to the separate structures

Figure 159 shows a comparison of the percentage distribution of single category's attacks with respect to the single structures with overall percentage distribution of accomplished attacks to separate structures. It is evident from the figure that the Critical Infrastructures are at the place before the last with respect to the accomplished attacks. In them, however, occurred almost equally effect of the two attacks' categories.

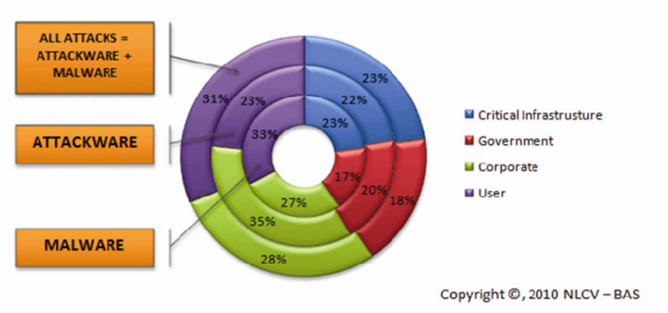

Figure 159. Comparison of the percentage distribution of single category's attacks with respect to the single structures with overall percentage distribution of accomplished attacks to separate structures

Table 10 shows the distribution of accomplished attacks by structures for each attack's group.

Table 10. Percentage distribution of accomplished attacks by structures for each attack's group.

Attack group	Total [%]	Government [%]	Corporate [%]	User [%]	Critical Infrastructure [%]
MALWARE					
Browser-related	7,06	1,48	1,27	1,84	2,47
Metadata	0,70	0,20	0,17	0,20	0,13
Cracking	1,41	0,38	0,17	0,51	0,35

Attack group	Total [%]	Government [%]	Corporate [%]	User [%]	Critical Infrastructure [%]
Spying	4,24	0,76	0,34	1,36	1,78
DoS, DDoS	7,77	1,32	2,49	2,17	1,79
Exploits	6,36	1,27	0,83	1,78	2,48
Scanners	2,12	0,53	0,30	0,59	0,70
Keyboard modifiers	3,53	0,35	0,49	1,38	1,31
Computer Trojan Horses	37,43	10,11	7,11	9,36	10,85
Computer Backdoors	5,65	1,92	0,62	1,36	1,75
Computer Worms	4,94	0,20	0,35	1,24	3,15
Computer Viruses	2,82	0,68	0,59	0,79	0,76
TOTAL MALWARE:	**84,03**	**19,21**	**14,72**	**22,57**	**27,53**
MALATTACKS					
Using accessible information	1,13	0,28	0,14	0,66	0,05
Overflow	2,57	0,67	0,36	1,21	0,33
Vulnerabilities	3,99	0,84	0,92	1,07	1,16
Content	0,29	0,07	0,07	0,07	0,08
Data Encapsulation	0,57	0,19	0,11	0,17	0,10
Denial of Service	3,14	0,75	0,85	1,13	0,41
Spoofing	1,42	0,30	0,34	0,41	0,37
CrackPasswd	0,86	0,21	0,14	0,24	0,27
Zombie Computers	2,00	0,24	0,18	0,64	0,94
TOTAL MALATTACKS:	**15,97**	**3,56**	**3,09**	**5,61**	**3,71**
ALL ATTACKS	**100,00**	**23,00**	**18,00**	**28,00**	**31,00**

Examined Critical Infrastructures include: Energy and Utilities; Communication and IT; Banking and Finance; Health care; Food and Agriculture; Water; Transportation; Safety; Government; Manufacturing.

With respect to individual objects' groups used in Software Critical Infrastructures, we can say that most attacks are carried out to Data, Internet related and Binary file objects (Figure 160, Figure 161).

Figure 162 shows the percentage distribution of accomplished attacks' groups which were carried out to all Critical Infrastructures.

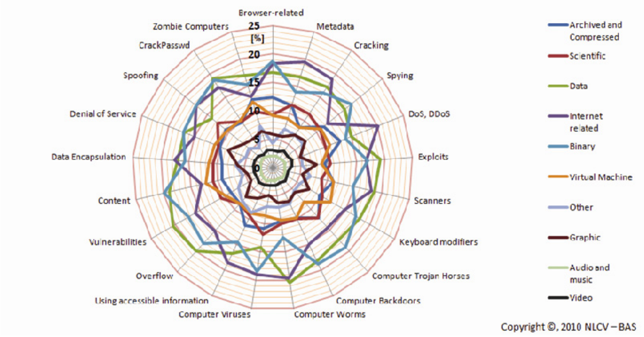

Figure 160. Percentage distribution of accomplished attacks groups to the Software Critical Infrastructures with respect to the objects' groups

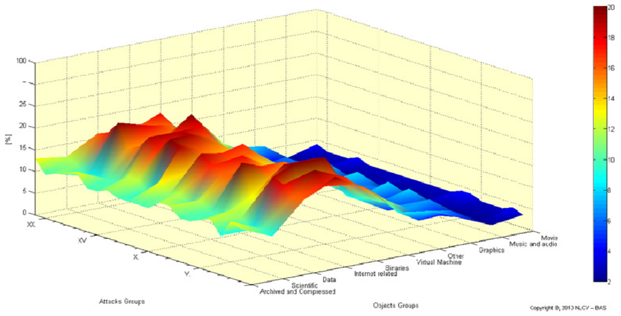

Figure 161. Percentage distribution of accomplished attacks groups to the Critical Infrastructures with respect to the objects' groups

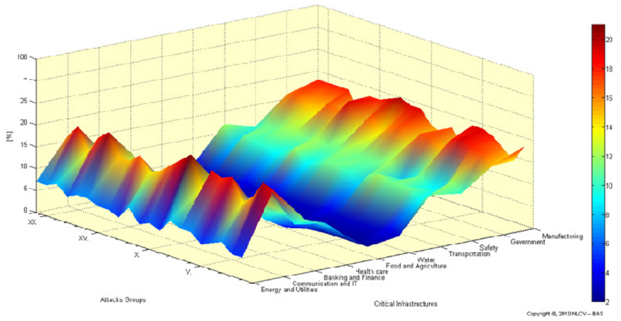

Figure 162. Percentage distribution of accomplished attacks groups to the Critical Infrastructures

9.4 Methods of prevention, protection and recovery

9.4.1 Methods of prevention

✓ **Human factor-related:**

– against disloyal employees or consultants;

- for loyal employees or consultants;
- against disloyal users;
- for loyal users;
- against disloyal system administrators;
- for loyal system administrators.

✓ **Media-related:**

- against theft;
- against copy/pasting;
- against physical harm/purposeful destruction;
- against copy/pasting (service maintenance).

✓ **Malware-related:**

- against viruses and the like;
- against future unauthorized access.

✓ **Related to electromagnetic emissions:**

- against screen information hijacking;
- against cable information hijacking.

✓ **Notebook related:**

- against unauthorized use;
- against theft.

✓ **Related to network topology:**

- against Internet effects;
- against network component manipulation.

✓ **Related to DoS attacks:**

Prevention of this type of attack is extremely difficult because it targets closed ports, can take different shapes, aims at many services and devices, and could be caused by legitimate packages if they cause a recursive effect such as opening and closing multiple simultaneous connections. A combination of the following is recommended:

- during network projection;
- for network perimeter protection.

✓ **Password related:**

- Use of strong password;
- Increase the length of the password (at least 8 symbols);
- Use of capital letters and numbers;

- Do not use personal information, names, whole words, easy to guess strings or hacker terminology in passwords;
- Do not write down passwords;
- Strict regulations regarding the number of stored used passwords (at least 10);
- Establishment of the minimum and maximum validity period of each password (0 days at least, 30 days at most);
- Use of password filtering programs such as passfilt.dll from Windows 2000 Resource Kit;
- Administrator testing with special password cracking tools;
- Complete ban on password sharing;
- Ban on password remembering of the program in question.

✓ **Virus related:**

- all of the software used should be bought from an authorized dealer;
- use of illegal software is unacceptable;
- all removable media (esp. those of unknown origin) should be scanned with an updated antivirus program;
- use of free publicly available software is to be avoided;
- floppy disks should be write-protected and removed from the computer when possible;
- if a non-virus protected Internet e-mail is used it should be done on an offline computer with updated antivirus.

✓ **Spam related:**

Spam blocking can be done on the mail server or the enduser's computer based on two models:

- black lists;
- contents filters.

✓ **Security policy related:**

According to SANS the security policy is viewed as a modular method for the development of specific targets or rules that are used to control the different aspects of a computer system such as password creation or real time application use. In brief, this document puts in writing how a company plans to defend its physical and informational assets.

9.4.2 Methods of protection

✓ **Basic functions**

The problem with absolute malignant software protection is practically impossible to solve but in order to protect a computer system we have to guarantee:

1) Intrusion protection

2) Resource inaccessibility

3) Inaccessibility of information in the working terminals

4) Cryptographic protection

✓ Basic tasks

The security protection of a company should have the following abilities.

1) Identify the attack.
2) Act on the attack.
3) Discover the attacks.
4) Reflect the attack.
5) Transparent work.

✓ Basic elements

The methods for computer system protection include the following basic elements:

1) Threat analysis.
2) Access control.
3) Authentication.
4) Confidentiality.
5) Data integrity.
6) Denial inability.
7) System reliability.

✓ Basic principles

The main principles for protection planning are:

1) Smallest privileges.
2) Deep protection.
3) Protection diversity.
4) Default denial.
5) Security by ambiguity.

✓ Basic methods

1) Data and file encoding
2) Methods for server antimalware protection
3) Methods for workstation antimalware protection
4) Methods for hoaxes protection
5) Methods for DDoS attack protection
6) Methods for protection against e-mail and spam bombings and IP spoofing
7) Protection against Sniffing
8) Protection against kernel level Rootkits
9) Protection against Smurf or Fraggle attacks

10) Protection against SYN Flood attacks

11) Protection against DNS attacks

12) Methods for wireless network protection

13) Methods for VPN protection

14) Methods for browser protection

15) Methods for mobile device protection (laptops, table computers, PDA etc.)

9.4.3 Methods of recovery

✓ Common preliminary measures

1) Strategy and recovery plan

The strategy and the plans should have clear and precise procedures for decision making regarding the people that should be informed about the incident the selection criteria for various recuperation procedures, supervisors, and responsibilities in order to prevent lengthy interruptions of regular activities.

The plan should include specific procedures for the different kinds of computer and network hardware, operating systems and application software.

The criteria and conditions on informing the authorities should also be included.

The final plan should be review by competent IT workers that did not participate in its development.

2) Concrete actions

- Creation of floppies and CDs for initial setup.
- A mail server for web-based back up should be installed outside the premises of the company for communication in case of a computer incident.
- Creation of backup e-mail accounts with global POP3 mail service sites.
- Installation of a backup Internet connection away from the organization's premises.
- Creation of an alternate site as an internal site (supported in a different location that has no connection to the mainframe), or as a Internet stored backup site.
- Frequent and complete backups.
- Backup storage in a secure place outside the computer system room as well as with Internet information storage sites.
- Backup storage on FireWire devices.
- Agreements to use office space at a different location in case of need.
- Gearing all IT employees and key workers with backup laptops in order to synchronize the main computer system restoration and not to interrupt the most important business activities.
- Backup system components ready for use in case of need.
- Standardization of the used hardware, software, and peripherals.
- The critical hardware components should be retail to avoid the delivery delay that comes with custom made equipment.

- Full documentation of system configurations and suppliers contact information for a quick switch in case of need.

✓ Preliminary measures for big computer systems

1) Constant updating off all critical databases.
2) Use of all fault-tolerant computer and network systems.
3) Use of extra components for critical systems.

✓ Preliminary measures for computer networks

1) Establishment of backup communication connections.
2) Use of several service providers.
3) Doubling of the devices creating the network connections.
4) Establishment of segmented networks.
5) Use of standard network technology.
6) Use of effective network security systems.
7) Use of all appropriate devices of network protections and prevention.

✓ Computer incident reaction methods

The various computer incident reaction methods include several different procedures. They all go through the following main stages.

1) Identification.
2) Qualification.
3) Limitation.
4) Source localization.
5) Target localization.
6) Deactivation.

✓ Computer system recovery methods

1) Coordination.
2) Review.
3) Evaluation.
4) Notification.
5) Description.
6) Shut down.
7) Removal.
8) Condition.
9) Recovery.
10) Return.

11) Check.

12) Guarantees.

✓ Recapitulation after recovery from the attack

Includes the answers to the following questions:

- How and why was there an attack?
- How were the consequences removed?
- Lessons that should be learnt for future reference.
- Having strictly determined goals that have quantified targets, deadlines and supervisors.
- Full documentation of the attack and the recuperation.
- Incorporating the necessary changes in the security policies and recuperation procedures to prevent future problems.

✓ Recovery after DoS attacks

DoS attacks require instant filtration measures depending on the nature of the attack. The traditional DoS attack usually does not cause host corruption, which makes recuperation extremely easy. If the client's IP address or the scheme of the attack can be quickly identified the traffic filtration in the router is easy to organize. The sophisticated DoS attacks as well as those committed by the Trojans Code Red and NIMDA, changed that perspective by damaging webhost platforms and generating different scanning and exploit schemes. Usually filtration is a temporary solution and it should be followed by the following to restore network services.

1) Access Control List (to limit malicious traffic).

2) Shut down of all unnecessary services.

3) Software update.

4) Fine tuning of Internet applications.

5) Eavesdropping services host access limitation through ACL.

In many cases the reaction and recuperation after a DoS attack requires intensive use of resources and bandwidth as well as close cooperation with the IPS to create a router filtering mechanism.

✓ Post-virus attack recuperation

The successful elimination of a certain virus from a computer system includes temporary restoration on removal of all infected or deleted files. The most effective way to restore damaged objects is to replace them with original copies. Thus, the frequent preparation of complete backup copies is very important and facilitates restoration.

After cleaning the virus from the computer system, it is necessary to scan all diskettes and other removable storage media to guarantee that they are virus-free. Should those measures not be performed a second infection of the computer system and the further distribution of the virus become a possibility.

9.5 Assessments

1. Sharp increase in the importance of security for Software Critical Infrastructures.

When establishing, Software Critical Infrastructure is required prior to making a roadmap for the movement of information flows between different components of the infrastructure. This can be described as follows:

1) Clarifying the number of the modules.
2) Clarifying the size of the modules.
3) Clarifying the number of the input, output, and input-output points for the information flows.
4) Reducing the number of the different points to one input-output point.
5) establishing a verifying mechanism that ensures the content of information flow during the input and output operation.
6) The verifying mechanism must be different for the input and output point.
7) Describing the duration as time for moving of information flow from point A to point B.
8) Adding additional time to perform supporting operations by certifying mechanism. A strict control during the movement of each information flow from point A to point B within the infrastructure is introduced by the roadmap.
9) Ensuring a relatively constant rate of movement of information flows through the overall management of the operating system.

2. Sharp increase in the price in establishing the Software Critical Infrastructures.

The increased requirements for how the infrastructure is created cause a significant increase in the price of its planning, the price of its creating and its using. This can be described as follows:

1) When planning, simulation experiments with different number of modules of the infrastructure, with different sizes of the modules and with different time and speed characteristics of the information flows, must be carried out.
2) Based on these experiments options in which to achieve the lowest price, average price and highest price, must be given.
3) Depending on the wishes of the client in the next phase of creating, an option is selected with respect to the three prices.
4) When creating the infrastructure is sought at an acceptable price in selected criterion for minimum, average, maximum price, while accomplishing an implementation of the prepared planning.
5) When using the infrastructure, an acceptable price is sought for the functioning of the infrastructure for certain periods such as microsecond, second, hour, day, month and year by managing the load of the infrastructure. The objective is to avoid peak values in energy consumption and repetitive processing of information flows.

3. Sharp increase in the complexity of establishing a Software Critical Infrastructures.

Increasing the number of the modules of the infrastructure, the number of the information flows and the long-term accumulation of recording information (logs) creates a condition for increasing the complexity of the infrastructure. This can be described as follows:

1) The number of the modules, their size, and the number of input-output points is directly related to the variants of running of the infrastructure whereby above a certain value of all

possible combinations mentioned above is reaching a level of complexity, which sharply aggravates the security of the Infrastructure.

2) The necessity of storing of recording information (logs) for the purpose of accomplishing of preventive and/or routine maintenance of the infrastructure, creates a critical threshold, which when is reached sharply aggravates the security of the infrastructure, because the ratio of useful and unnecessary information is changing catastrophically.

4. Sharp increase in vulnerabilities in the creation of Software Critical Infrastructures.

Security issues in the creation of the infrastructure have one side, but very important effect, namely, is ever increasing the vulnerabilities in the infrastructure. This can be described as follows:

1. The lack of sufficient time for completely full examination of possible combinations for connecting the modules, their sizes, the number of input-output points, the number of information flows, their speed and the number of the repetitions in the processing of the content of information flow leads to omissions in pre-planned functioning of the infrastructure. These omissions are the basis for the beginning of so-called infrastructure vulnerabilities.
2. The existence of free computational resources with a large number of processors and much more core numbers in these processors allows authors of attacking tools to receive serious advantage in the detection of vulnerabilities and their use for accomplishing attacks to the infrastructure.

9.6 Discussion

The problems of the Software Critical Infrastructure can be summarized as follows:

1. A change in the funding rules for establishing the infrastructure towards increasing the percentage of financing of test procedures and policies.
2. A change in the rules for scheduling for creating the Infrastructure in favor of increasing the percentage of the time for test procedures and policies in case of fully loading of the Infrastructure.
3. A change in the rules for individual modules, groups of modules and groups of software tools, composing the infrastructure in favor of adding a component to an existing configuration, only in case of fully one hundred percent completed testing procedure and policy.
4. A change in the rules for searching, detecting and correcting of vulnerabilities in favor of generous funding for each discovered vulnerability within the developer team, or forming a special team for discovering vulnerabilities with special funding for newly discovered single vulnerability.

In this connection in necessary to increase the funding, to create new methods for reducing the complexity of the Infrastructure and new methods for reducing the vulnerabilities to ensure the adequate security in creating of Software Critical Infrastructure.