

From Network and Information Security Situation Analyse to Incidents Management

Rytis Rainys

Network and Information Security Division
Communications Regulatory Authority of the Republic of Lithuania
Algirdo St. 27, LT-03219 Vilnius, Lithuania
e-mail: rrainys@rrt.lt

Abstract—The studies, executed in Lithuania have shown that 85% of the Internet users, 79% of enterprises and 100% of the ISPs face computer viruses and spam. This forces to view the situation systematically and immediately react by developing separate security incidents management mechanisms. Author suggest CERT model that can quickly respond to the security incidents in networks, analyze them and coordinate the incident elimination activities, especially when there is a potential risk to the functionality of the network or security of the data.

Keywords—component; network and information security, security incident, CERT.

I. INTRODUCTION

The article seeks to cast a broad look to the issues of electronic security, distinguishing main threats to security and finding the measures to effectively deal with the problem. Since IT development is very intensive, these issues are particularly important to Lithuania. After some time we are going to face much more complex security problems, which, if unresolved, will bring heavy losses for businesses, state institutions, home users, and individual specialists who will be unable to avert the problems.

The influence of security incidents on electronic communications networks is constantly growing and it may be forecasted that in the future there will be much more incidents. Security threats are determined by the following main reasons:

The Internet network (TCP/IP protocol) not adapted to high level security requirements, complexity of information systems (e-commerce, e-banking, e-government, SCADA), shorten time of security attacks exploitation, financially motivated objectives of cyber-criminals', botnet networks – these are the main reasons of threats to network and information security.

II. SURVEY

Main existing threats (although the list is far from complete) to security of electronic communications networks also exist in Lithuania and the extent of the impact to Lithuania's Internet users may be demonstrated in special studies.

Up to now there has been no deep survey performed to identify networks and information security situation in Lithuania. In the end of 2005, the author carried out a special

survey aiming to identify the main problems of networks and information security faced by the Internet users and to evaluate the scope of the said problems in Lithuania. 1386 home Internet users, 500 enterprises and 31 Internet service providers (hereinafter referred to as ISPs) were surveyed.

1. The first objective was to identify the types of security incidents, faced more frequently and their scope. The study demonstrated that the major part of users face computer viruses and spam. Taking into consideration that during 20 years of computer viruses' existence approximately 150 000 viruses have been created and the fact that at present spam reaches 70% of the total volume of e-mail, the results are not surprising. However, 44% of ISPs have to withstand the denial of service attacks against their servers and computers, which potentially brings a greater destructive effect than other incidents, since they are often executed by using the botnet networks.

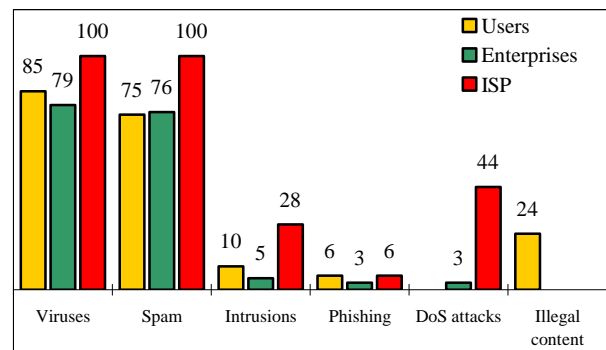


Figure 1. The security incidents, faced by the users (per cent)

2. The next step was to identify security tools used. The tool, most frequently used by the Internet users for safeguarding against the security incidents, is a anti-virus program, designed for protection against computer viruses. The study has shown that the ISP also uses other security tools, for instance anti-spam, anti-spyware, firewalls and intrusion detection systems (IDS) quite actively. This can be explained by the fact that, as actually the entire Internet flow passes via the systems of ISP, they become more frequent targets for attacks, therefore, it is natural that the ISPs are the most active users of security tools. Attention should be also drawn to the fact that home users and enterprises too rarely

use continuous upgrading of operational systems (hereinafter referred to as OS), which is the critical factor in order to ensure security, since it is the OS security gaps, which most often result in security incidents (viruses, spyware, etc.) The figures are 46% for home users and 33% for enterprises, respectively).

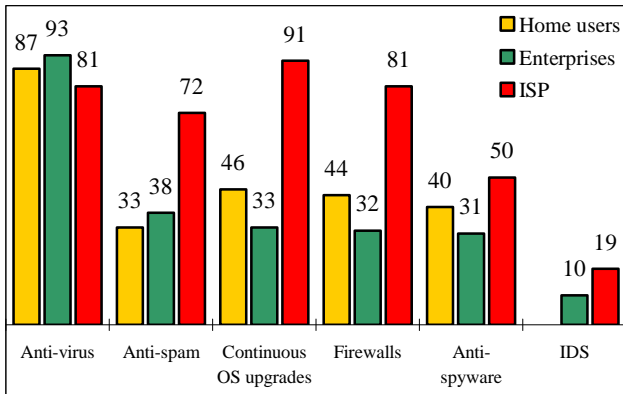


Figure 2. Usage of security tools (per cent)

In comparison with the UK survey [1], usage of safeguard tools is bigger in UK: 98% have anti-virus, 86% have anti-spam, 83% upgrade OS, 74% have anti-spyware and 48% IDS.

3. The previous study has shown that the majority of users face different security incidents and use different security tools (to different extent). However, does such security suffice? Unfortunately, another study showed that a good deal of the Internet users suffer from threats to security (Figure 3). 27 % of home users, 25 % of enterprises and even 68 % of ISPs incurred certain damage.

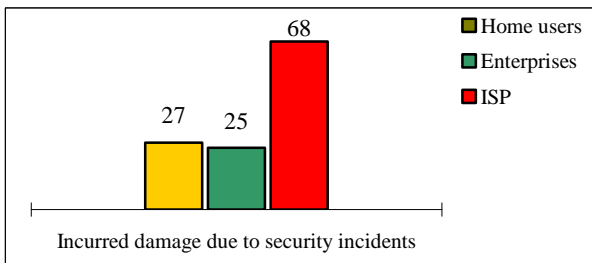


Figure 3. The users, incurring damage due to security incidents (per cent)

In comparison with the UK [1], 35% of enterprises in UK incurred damage due to security incidents, that is 10% more than in Lithuania.

4. When identifying the character of the damage, incurred due to security incidents, it was established that most often the loss is related to the damaged software, which was specified by 70% of home users, 43% of enterprises and 41% of ISPs (Figure 4). Normal activities of the organization were disrupted in approximately half of enterprises and ISPs.

The study of networks and information security in Lithuania illustrates that the users of the Internet/electronic communications face lots of security incidents, incur damage and insufficiently use security tools. It forces to look at the

situation in a systematic manner, respond to it immediately and develop mechanisms for management of security incidents.

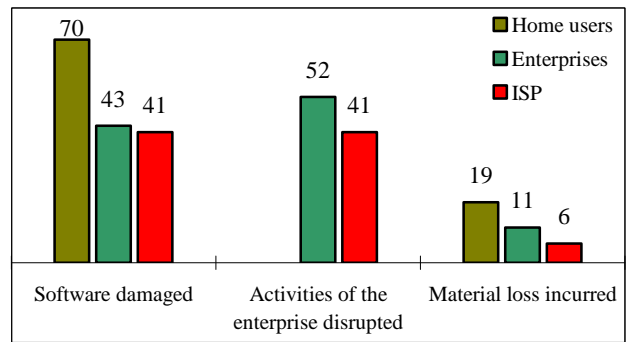


Figure 4. The type of damage, incurred due to incidents (per cent)

III. SECURITY INCIDENTS MANAGEMENT

It is practically impossible to reach absolute security of a computer, information system or a network. Security is the target, which must be strived all the time. CERT (Computer Emergency Response Team) is the organisational model for networks and information security incidents management.

Under the CERT model, the management of security incidents is carried out in three basic stages: 1) receipt, evaluation of the incident reports and the initial prioritization (assortment); 2) study and technical handling of the incidents and informing target groups of users on the threats; 3) response to incidents, statistical registration, prevention of spreading incidents, network function restoration [1].

In a functioning CERT, close interconnection between the aforementioned stages (functional objects), exists which is shown in Figure 5. The directions, shown in bold, are basic, they show the direction of the main work on the incident. The early warning system, i. e. a preventive tool used to inform target groups (users, network administrators, other CERT) in order to prevent further spreading of incidents, plays an important role.

The main handled object within the CERT activity model is the security incident itself. The specific procedure of handling the incident is an individual decision of each CERT service. In the future, by applying the classic CERT model framework, the author is going to attempt to develop an individual variant of handling the incident, acceptable in the situation of Lithuania's Internet networks.

Therefore, the information on the incident, after being received by the CERT, passes through the entire cycle of handling inside the CERT system, which is simple to convert into an elementary algorithm, shown in Figure 6. The life cycle of incidents within the CERT model can be analyzed by the following stages:

1. First, a report on a security incident is received. This can be done by e-mail, telephone, to a web-site or by IDS. The confidential information is forwarded by using the electronic signature technology (asymmetric cryptography). The

received report is registered by using the special incidents management program, which assigns the incident an individual identification number, which remains the same throughout the entire process till the closing of the incident.

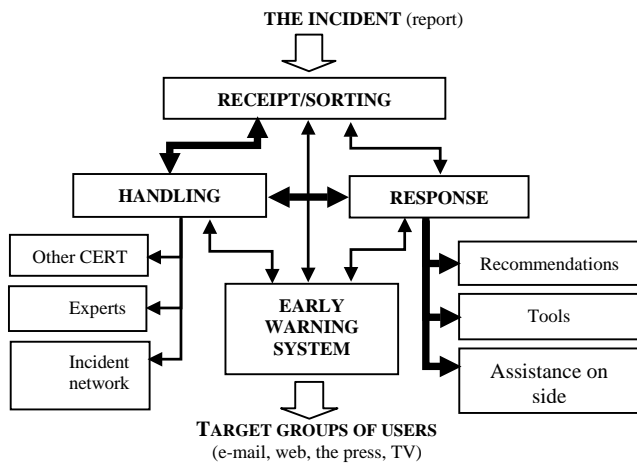


Figure 5. The functional diagram of the activities of CERT

2. During the following phase the level of danger of the incident to security is evaluated, i. e. the security category is assigned. When evaluating the following factors are taken into consideration: a) destructive effect of the attack (is it for example commercial spam or a virus, changing the structure of files); b) the importance of the affected computer system (is it a server, providing the service to multiple customers or a periphery network equipment that was attacked); c) the extent of the spread of the incident (how fast the incident is spreading; is it still active). The time for reaction by the CERT depends on the assigned category. The incident of the highest category of course shall be handled immediately.

3. When needed, preventive measures are taken. In case the incident is in progress and it is not possible to stop it locally and other users may be affected, the IP address of the source of the incident is blocked or attempts to disconnect from the botnet network are made, etc. When the incident is dangerous and brings the risk of further hazard, the warning to network users and other CERT groups is prepared.

4. After the mentioned actions the CERT staff, with the help of special hardware and software analyzes the content and environment of the incident, collects statistic data and develops security tools. That is the cycle of execution of the actions, shown in Figure 6:

a) Analysis of the incident is the main action of the CERT. The following can be analyzed: the incident logs file, the incident itself (for instance, malicious programming code), the hardware and/or software, in the environment of which the incident occurred. Analysis of log files often becomes the main object for analysis, since it can show the configuration of the system, in which and the time when the incident was registered, which processes within the system were disrupted, etc. In case the incident spreads itself as a separate process within the network (e. g. a virus), it should be analyzed

separately. In this case a virtual isolated computer environment is created, in which the virus is activated and the special programs can monitor and register the changes, made by the virus in the system. The control quantum can show the changes, and thus the damage is evaluated and the safeguarding options are considered.

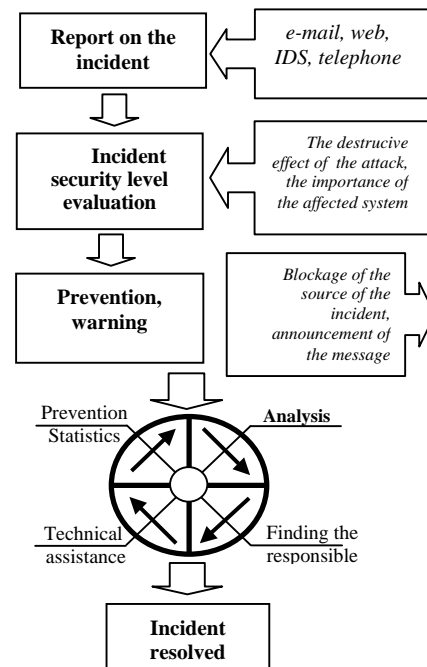


Figure 6. Life cycle of a security incident

b) After a thorough analysis of the incident, the persons, responsible for the incident are traced back therefore the IP address of the source of the incident is analyzed. The person, responsible for the incident is found via the internal and external databases (for instance, the international *whois* system), in case of a need the initiator of the incident is warned to stop the incident and, in case the incident comes from another country, the CERT, acting in the network of that country is informed. On the other hand it is necessary to know the coordinates of the incident reporter precisely in order to be able to receive additional information, in case that is necessary for analysis.

c) In case the incident spreads further to other networks, the security tools must be developed and implemented as soon as possible, in order to minimize the possible damage. In case the incident does not spread, however the systems experience a destructive effect, the CERT service takes the actions in order to develop the corresponding recommendations or technical tools, able to recover the system back to the previous state.

d) The collected information can be passed over to the institutions of law and order (cyberpolic), in case an administrative or criminal amenability is foreseen for rising of the incident according to the laws. In any case the incident is statistically registered in order for the general trends of

coming into existence of incidents to be continuously monitored.

5. In case the mentioned actions bring no result, i. e. the reasons for the incident remain unclear, the spread is not stopped, the destroyed network or system segments are not recovered, the incident is returned to the analysis stage. Otherwise the incident is held resolved and is closed.

Apart of the main activities, related with responding to the IT security incidents, the CERT executes preventive actions by systems vulnerability researches. The CERT also analyzes the statistical data, communicates the information and the results of investigations to the operational institutions (the electronic space crime investigation department) and other domestic and international CERT groups.

IV. SYSTEM IN LITHUANIA

The survey, executed in 2005 showed that only 17% of ISP have introduced units, corresponding to the CERT model in their networks, although a significant part of ISP (49%) handle incidents only when they occur. However the remaining part (34%) is in essence not ready to handle security incidents [3], which means that a significant part of Lithuania’s Internet users is not safeguarded against the danger, raised by security incidents. In addition, there is a risk that the incidents, coming from such networks will not be prevented.

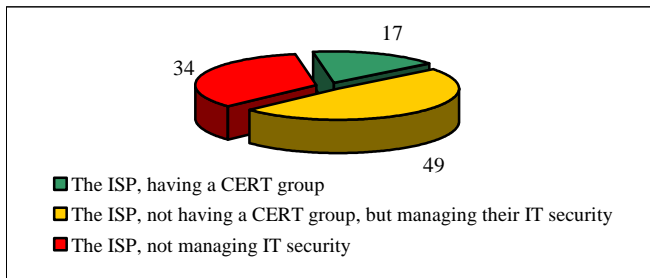


Figure 7. Implementation of the CERT model (per cent)

Taking the situation into consideration, the conclusion can be made that different Lithuania’s Internet networks have different security level, which brings negative effect to the general networks and information security situation therefore it is necessary to develop a CERT service (let us call it CERT-ISP), the activities of which would cover the part of the Internet networks, in which no management of security incidents is executed. The CERT-ISP would respond to security incidents and coordinate common ISP actions on fighting networks and information security incidents. The ISP Sector is a critical spot in safeguarding against security incidents. So the major task of CERT-ISP work should be to cover this 34 % “white spot” of ISPs networks that are not able to handle security incidents. This activity should improve and compare overall security situation.

However that is not enough to reach the optimum incidents management on the country level. Separate CERT teams need a coordination centre, which would be an official common contact point for resolution of international and inter-network incidents and coordination of common actions, taken in order to ensure security of networks and information. Basically a hierarchical CERT service unit’s structure, shown in Figure 8 should be introduced in Lithuania. The information and decision taking would continuously circulate between the shown CERT levels. It should bring an effect of reaching secure and reliable networks and information.

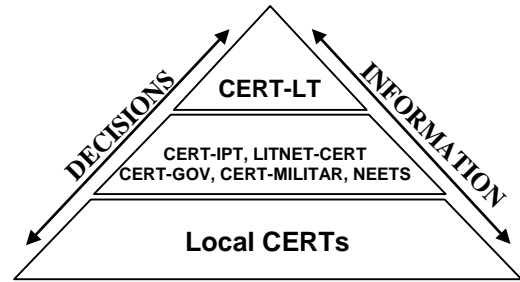


Figure 8. The CERT hierarchy in Lithuania (per cent)

V. CONCLUSIONS

An increasing usage of information technologies results in bigger threats. It is necessary to draw attention to the increasing number of incidents in virtual space and the growing professionalisms of perpetrators. In author point of view, CERT model is most effective model to manage security incidents on national level.

To summarize, it can be clearly stated that the role of CERT in striving for security of networks and information is huge. The CERT service units are the backbone, around which the networks and information security activities should be developed, since it is the CERT that is able to see the bigger picture of networks’ security and could quickly respond to incidents.

In case efficient management of security incidents in the networks of ISP is ensured, there will be no need to resolve the security problems at the Internet users’ level. That is why the activities of CERT-ISP service in Lithuania should be efficient to the maximum

REFERENCES

- [1] UK Department of Trade and Industry, <http://www.pwc.com/Extweb/pwcpublishations.nsf/docid/F9843CD3C8E0FB828025715A0058C63B>, August 2006.
- [2] Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd Edition: April 2003.
- [3] The Communications Regulatory Authority of the Republic of Lithuania, <http://www.esaugumas.lt>, August 2005.