ELECTRONCS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2006. Nr. 6(70)*
ELEKTRONIKA IR ELEKTROTECHNIKA

TELECOMMUNICATIONS ENGINEERING
T 180
TELEKOMUNIKACIJŲ INŽINERIJA

Network and Information Security. Assessments and Incidents Handling

R. Rainys
Networks and Information Security Division, Market Surveillance Department, Communications Regulatory Authority of the Republic of Lithuania,
Algirdo str. 27, LT-03219 Vilnius, Lithuania, phone: +370 5 2105 76; e-mail: rrainys@rrt.lt

Introduction

Mankind's continuous quest for knowledge and the advance of telecommunications has stimulated the development of electronic communications up to the present level, with the Internet becoming the most powerful and most broadly accessible form of communication.

In the 21st century major part of social relations is moving to the virtual space. People use electronic communications ever more actively not only for finding important information on the web, but also for ordering and purchasing goods, paying for utility services and transferring money electronically. Government institutions, on the other hand, are searching for more ways to provide their services via the Internet and to reduce their costs businesses often go online.

In 2005 the number of Lithuania's households, owning computers reached 29 %, and the number of regular Internet users, reached 781 thousand by October 2005. Statistical comparison allows seeing a 2.6 times annual increase in the Internet usage in the country. The said indicator is one of the highest in Europe at the moment [1].

Unfortunately together with social relations criminal activities have also moved to the virtual space. Surveys (see the "Surveys" chapter) shows that ever more often users of electronic communications face phishing of confidential information, intrusions to information systems, computer viruses, increase of spam, DoS attacks and other problems, related with the security of networks and information.

An increasing usage of information technologies results in bigger threats. Since the possibilities of information technologies (hereinafter referred to as IT) are going to develop in the future, one of the major problems in the sphere, - ensuring security, can not be ignored. It is necessary to draw attention to the increasing number of crimes in virtual space and the growing professionalisms of perpetrators.

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 for Lithuania; after some time we are to face bigger and a whole lot more complex security problems, which if unresolved will translate into major losses for businesses, state institutions and home users and individual specialists will be unable to avert the problems.

Threats to Security

General analysis of the situation, involving various security incidents, spreading via the Internet and studies on the state of affairs Lithuania paint a rather threatening picture of networks and information security. Today almost every IT user faces security of networks and information threats. The influence of security incidents to electronic communication networks is constantly growing and it may be forecasted that in the future there will be a whole lot more incidents. Security threats are determined by the following main reasons:

1. The Internet network, developed and improved back in the sixties, was not adapted to high level security requirements, which have become extremely important these days. What the academia needed at that time was just a simple and universal network standard, connecting different types of digital calculation equipment into a common data transmission network. Later on the network was used to connect separate data communication networks, which was realized by the TCP/IP (*Transmission Control Protocol/Internet Protocol*). The Internet has spread throughout the world at a lightning speed, therefore at present, as large security problems have come into existence, it is practically impossible to replace it by another and more secure network. There are millions of information systems connected to the Internet and there may be billions of network equipment units manufactured for operation in TCP/IP networks. It would be extremely

difficult for users to replace the whole of technical equipment therefore it is quite natural, that manufacturers are not interested to do that. Therefore there is a need to search for other networks and information security control mechanisms.

2. Complexity of information systems is increasing: business systems goes online (so called e-commerce), banking operations are moved to the Internet (e-banking); government institutions are also moving their services, provided to the people to the electronic space (e-government); the SCADA (*Supervisory Control And Data Acquisition*) systems are functioning on the web, etc. Due to such complexity of information systems and their integration with the Internet the systems become more complex and this increases the risk of more security loopholes coming into existence (which unavoidably happens).

3. Extensive programs, consisting of a huge number of programming code lines are developed to service modern complex computer systems. Experts reckon that 1000 programming code lines contain from 5 up to 20 errors. Popular network management operational systems consist of approximately 35 million programming code lines, which means that they may potentially contain from 175 000 up to 700 000 programming errors (security gaps). This once again illustrates the existing threats to electronic security.

4. It is observed that security gaps shorten time of security attacks. For instance, in 2000 the *Nimba* virus used a security gap in the *Microsoft* operational system, detected a year before, and the creation of the *Sasser* virus in 2004 took just 17 days. In the same year the *Witty* virus was created in 1 day after vulnerability of the software was discovered and reported [2]. The trend is obvious and ever less time is left to respond to security incidents.

5. It can be noticed that the objectives of cyber-criminals' attacks are changing, these days they are motivated financially. If some time ago all hackers wanted was to become famous or maliciously bring damage to somebody, today financial benefits are becoming their ultimate goal. For instance, at present computer viruses most often act invisibly to the user, and the performance of the computer system remains almost unchanged while the virus collects the information, which later is used for financial crimes. Alternatively one can order a computer attack against a business competitor via the Internet (by denial of service). Due to an actual financial damage, the situation becomes even more dangerous.

6. *Botnet* networks, i. e. the networks, consisting of damaged computers, managed remotely via the controllers are a major problem, since the networks can connect up to several thousand of computers. In case they are directed to a selected target, they can bring far more harm than isolated attacks.

7. With attacks targeting mobile telephones or palmtops mobility of security incidents may also be observed. There are more than one billion of mobile telephones in the world (far more than computers) therefore in the near future attacks may target mobile telephones, which will bring damage to an even bigger target group. During 2005 the research laboratory of the McAfee enterprise has studied 226 mobile viruses and the security specialists of the said company forecasted that 2006 can bring even more mobile viruses and the number can reach 726 [3]. There are reasons to believe that the number of mobile viruses is going to increase continually.

Surveys

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.

In the end of 2005 the RRT carried out a special survey aiming to identify main problems of security of networks and information 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 ISP) 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 the 20 years of existence of computer viruses 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 ISP has to withstand the denial of service attacks against their servers and computers, which potentially bring a greater destructive effect than other incidents, since they are often executed by using the *botnet* networks.

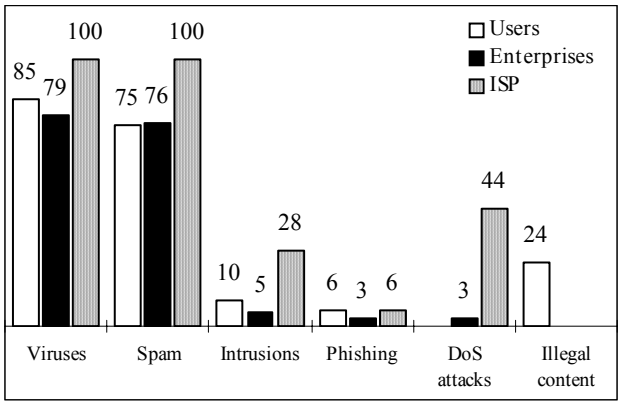

Fig. 1. The security incidents, faced by the users (per cent)

2. The next step was to identify security tools the used. The tool, most frequently used by the Internet users for safeguarding against the security incidents is anti-virus programs, designed for protection against computer viruses. The study has shown that the ISP also use 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 only natural that the ISP are 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, correspondingly).

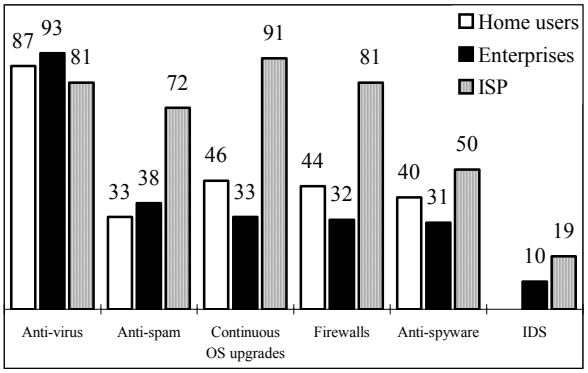

Fig. 2. Usage of security tools (per cent)

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

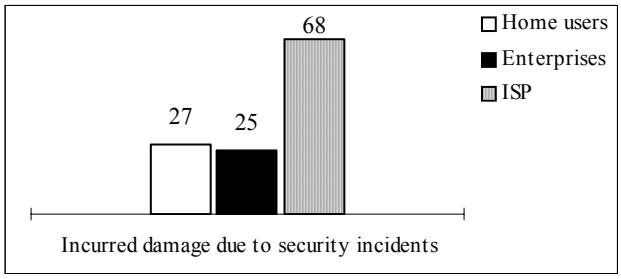

Fig. 3. The users, incurring damage due to security incidents (per cent)

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

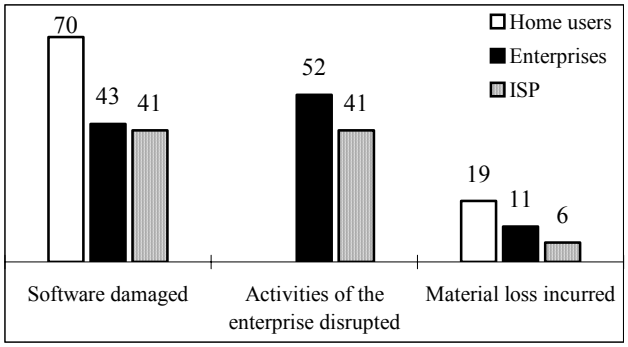

Fig. 4. The type of damage, incurred due to security incidents (per cent)

This study of networks and information security in Lithuania illustrates that the users of the Internet/electronic communications face lots of security incidents and incur damage and display an insufficient usage of 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.

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) specifically contributes to the implementation of the said target.

CERT, also known as CSIRT (Computer Security Incident Response Team) is the service, responding to networks and information security incidents, the main target of which is to quickly respond to security incidents in electronic communications networks, study the incidents and coordinate the actions when eliminating the incidents, especially when there is a potential risk to functionality of the network or security of the data. In other words, CERT is a kind of fire brigade in the electronic space.

The history of CERT began in 1988, when one of the first Internet worms (a variety of virus, which disseminates itself inside the network) travelled throughout the worldwide web and interrupted the activities of most systems. In the same year the first CERT model was developed (the IT security incidents research group) and registered in the US Patent Office and is still functioning in the Carnegie Mellon University. The CERT activity model, developed in the academic sector was a successful idea and became the most important tool for management of IT security incidents in the electronic communication networks. At present there are several hundreds state, commercial and academic CERT of different size in the world.

The CERT Model

Under the CERT model, the management of security incidents is carried out in three basic stages [4]:

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 of incidents, network function restoration.

In a functioning CERT, close interconnections exist between the aforementioned stages (functional objects), which are shown in Fig. 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 of the incident is the individual decision of each CERT service. In the future, by applying the classic

CERT model framework we are going to attempt to develop an individual variant of handling of the incident, acceptable in the situation of Lithuania's Internet networks.

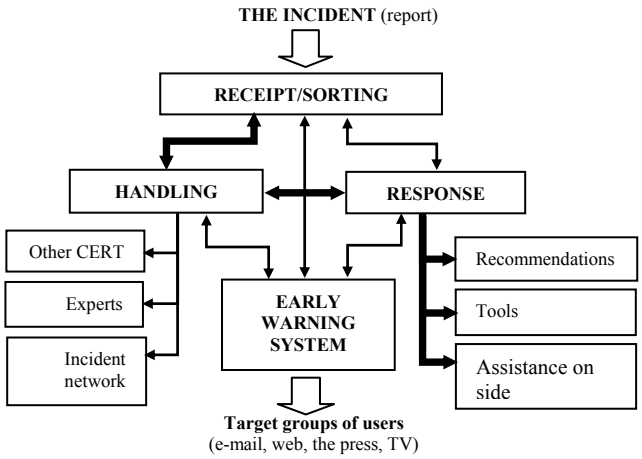

Fig. 5. The functional diagram of the activities of CERT

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 Fig. 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.

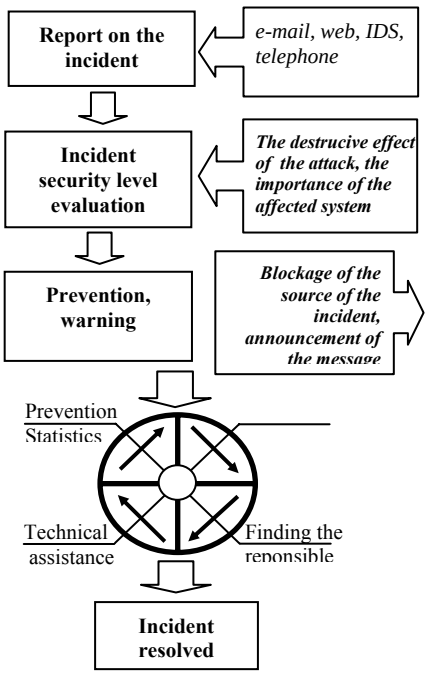

Fig. 6. Life cycle of a security incident

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 (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 in progress?). The time for reaction by the CERT depends on the assigned category. The incident of the highest category 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 Fig. 6:

a) Analysis of the incident is the main action of the CERT. The following is analyzed: the incident log file, the incident itself (for instance, malicious programming code), the hardware and/or software, in the environment of which the incident occurred. Each operational system (especially that functioning in servers) has tools for registering the system's errors and storing them in special log archives. 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 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.

b) After a thorough analysis of the incident, the persons, responsible for the incident are traced back therefore the IP (internet protocol) 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 network equipment, the security tools must be developed and implemented as soon as practicable, 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, in case an administrative or criminal amenability is foreseen for raising 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.

Usually, apart of the main activities, related with responding to the IT security incidents, the CERT executes preventive actions by providing the information on the new IT security problems and the potential threats to the functioning of the IT systems or computers to the users. 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, induces to found local CERT.

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 big picture of networks' security and quickly respond to incidents.

The CERT 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 [1], 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.

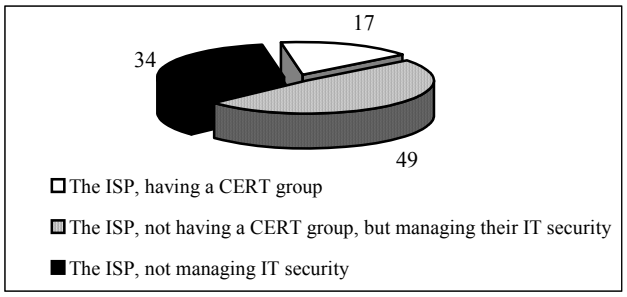

Fig. 7. Implementation of the CERT model (per cent)

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. 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.

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 Fig. 8 should be introduced in Lithuania. The information and decision taking would continuously circulate between the shown CERT levels.

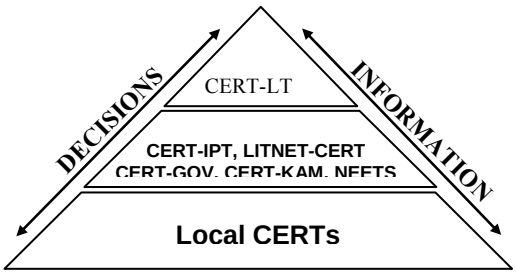

Fig. 8. The CERT hierarchy in Lithuania (per cent)

It should bring an effect of reaching secure and reliable networks and information.

References

1. **The Communications** Regulatory Authority of the Republic of Lithuania, http://www.esaugumas.lt
2. **European Networks** and Information Security Agency, http://www.enisa.eu.int
3. **Kawamoto D.** 2006 – Year of the mobile malware. – **CNET** news, December 19, 2005. Access on internet http://news.com.com/2006+Year+of+the+mobile+malware/2100-7349_3-6001651.html
4. **Handbook** for Computer Security Incident Response Teams (CSIRTs), 2nd Edition, April 2003.

Submitted 2006 01 03

R. Rainys. Network and Information Security. Assessments and Incidents Handling // Electronics and Electrical Engineering. – Kaunas: Technologija, 2006. – No. 6(70). – P. 69–74.

The TCP/IP, not adapted to the high security requirements, the ever increasing complexity of information systems, security gaps in the software and the shorter time for elimination of incidents, occurring due to the software gaps, financial motivation of cyber-criminals, the botnet networks and mobility of the security incidents show a rather threatening networks and information security situation in the world. The studies, executed in Lithuania in 2005 have shown that 85 % of the Internet users, 79 % of enterprises and 100 % of the Internet services providers (hereinafter referred to as ICP) face computer viruses and spam. This forces to view the situation systematically and immediately react by developing separate security incidents management mechanisms and CERT crews. The aim of CERT is to quickly respond to the security incidents in the electronic communication 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. After ensuring the efficient management of security incidents in the networks of Lithuania's ISP, there would be no need to resolve the security problems at the Internet home users' level. That is why the development and activities of a CERT-IPT service in Lithuania should be efficient to the maximum. Il. 8, bibl. 4 (in English; summaries in English, Russian and Lithuanian).

Р. Райнис. Безопасность сетей и информации. Аттестация и управление инцидентами // Электроника и электротехника. – Каунас: Технология, 2006. – № 6(70). – С. 69–74.

TCP/IP протокол, который не соответствует высоким требованиям безопасности, возрастающая комплексность информационных систем, бреши безопасности в программном обеспечении и укорачивающийся срок, когда они используются для выполнения инцидентов безопасности, финансовая мотивация кибернетных преступников, сети botnet и мобильность инцидентов безопасности иллюстрируют достаточно грозную ситуацию безопасности сетей и информации в мире. Исследования 2005 года в Литве показали, что 85 % пользователей интернета, 79 % предприятий и 100 % поставщиков услуг интернета (ПУИ) сталкиваются с компьютерными вирусами и спамом. Это заставляет систематично посмотреть на ситуацию и реагировать немедленно, создавая отдельные механизмы управления инцидентами безопасности, службы CERT. Цель CERT – оперативно реагировать на инциденты безопасности в электронной сети связи, выполнять их исследования и координировать действия при их удалении, особенно когда есть потенциальный риск для функциональности сети или безопасности данных. Обеспечив эффективное управление инцидентами безопасности в сетях ПУИ Литвы, ненужным стало бы решение проблем безопасности на уровне рядовых пользователей интернета. Вот почему создание в Литве службы CERT-IPT и ее деятельность были бы максимально эффективными. Ил. 8, библ. (на английском языке; рефераты на английском, русском и литовском яз.).

R. Rainys. Tinklų ir informacijos saugumas. Atestacija ir incidentų valdymas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2006. – Nr. 6(70). – P. 69–74.

Nepritaikytas aukštiems saugumo reikalavimams TCP/IP protokolas, didėjantis informacinių sistemų kompleksiškumas, programinės įrangos saugumo spragos ir trumpėjantis laikas, kai jos panaudojamos saugumo incidentams įvykdyti, kibernetinių nusikaltėlių finansinė motyvacija, „botnet“ tinklai ir saugumo incidentų mobilumas atskleidžia gana grėsmingą tinklų ir informacijos saugumo situaciją pasaulyje. 2005 metų tyrimai Lietuvoje parodė, kad 85 % interneto vartotojų, 79 % įmonių ir 100 % interneto paslaugų teikėjų (IPT) susiduria su kompiuteriniais virusais ir elektroniniu šiukšlinimu. Tai verčia į situaciją pažvelgti sistemiškai ir nedelsiant reaguoti kuriant atskirus saugumo incidentų valdymo mechanizmus, CERT tarnybas. CERT tikslas yra operatyviai reaguoti į saugumo incidentus elektroninių ryšių tinkle, vykdyti jų tyrimus ir koordinuoti veiksmus juos šalinant, ypač kai yra potenciali rizika tinklo funkcionalumui ar duomenų saugumui. Užtikrinus efektyvų saugumo incidentų valdymą Lietuvos IPT tinkluose, nebereiktų spręsti saugumo problemų eilinių interneto naudotojų lygmenyje. Todėl Lietuvoje būtina sukurti efektyviai veikiančią CERT-IPT tarnybą. Il. 8, bibl. 4 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).