



DIRECTION TO SUCCESS. PUBLIC AND PRIVATE SECTORS PARTNERSHIP

WSIS Action Line Facilitation Meeting:
Building confidence and security in the use of ICTs (C5)
“Partnerships for Global Cybersecurity
ITU Geneva, 15-16 May 2006

Outline of the presentation



- @ Challenges in network and information security
- @ NRA actions area
- @ Direction to success: public and private sectors partnerships
- @ Conclusions

Majority of social relations is moving to the virtual space

People use electronic communications ever more actively not only for finding important information on the Internet, but also for ordering and purchasing goods, paying for utility services and transferring money electronically.

Developments in electronic devices and data transfer technologies allows connectivity to services anywhere, anytime.

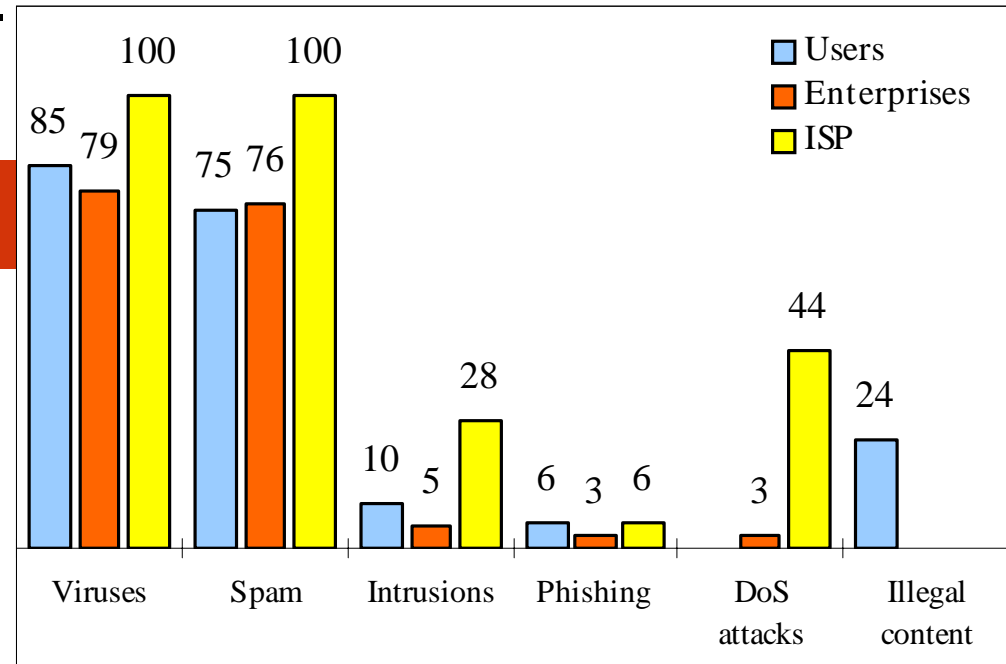
Unfortunately, together with social relations criminal activities are also moving to the virtual space.



Survey aiming to identify main problems...

The study demonstrated that the major part of users face computer viruses and spam.

...Lithuanian case

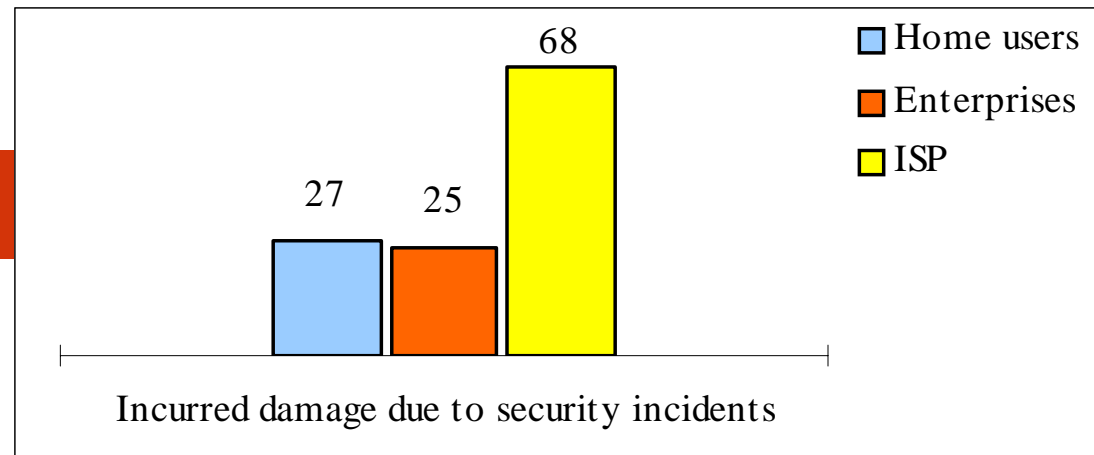


Taking into consideration that during the 20 years of existence of computer viruses approximately 150.000 viruses have been created and the fact that at present spam reaches 80% of the global e-mail volume, the results are not surprising.

Survey aiming to identify main problems...

Despite the fact, that majority of users employ different security tools, the quarter of home users and enterprises and most of ISPs suffer from threats to security.

...Lithuanian case



Since all the Internet stream goes over ISPs networks, they naturally incur the biggest damage of security incidents.

Current challenges in network and information security



- @ Increasing complexity of networks and software;
- @ Internet has been created without security in mind;
- @ Lack of cross-jurisdictional regulatory measures;
- @ Critical infrastructures linkage to relatively insecure networks;
- @ Security underestimation in building of new technical platforms;
- @ Users themselves are responsible for vulnerability of the system;
- @ IT security balance with issues such as interoperability, privacy and ease of use.

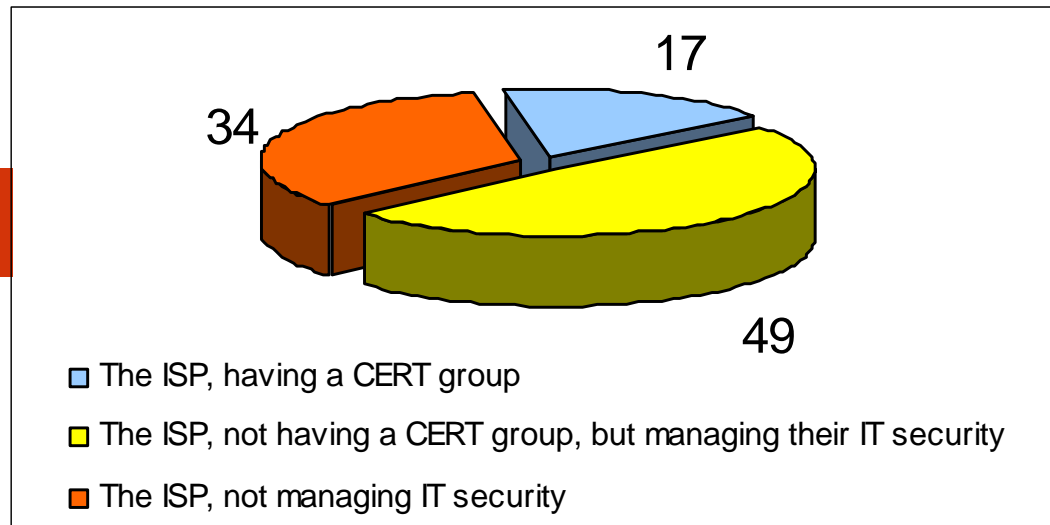
- @ Objective – secure information society:
- **Execution of CERT functions;**
 - **Rising of consumer awareness;**
 - **Reduction of security incidents negative impact;**
 - Enhancement of legal and standardization measures;
 - Drafting law on electronic communication networks and information security in Lithuania;
 - Inter-institutional and international cooperation;
 - Staff training;
 - Monitoring of network and information security situation.

Survey aiming to identify Lithuanian CERT map



The survey, executed in 2005 showed that only 17% of ISP have introduced CERT units, 49% handle incidents only when they occur and the remaining part (34%) is in essence not ready to handle security incidents.

...Lithuanian case



Different Lithuania's Internet networks have different security level, which brings negative effect to the general security situation

Specific actions: CERT functions

- @ **ISP Sector is a critical spot.** If efficient management of security incidents in the networks of ISP is ensured, there will be no need to resolve the security problems at the users' level.

- @ Government resolution of 24 March 2005 projects creation of CERT within RRT till the end of 2006:
 - **coordination** of incidents' investigation and response to them;
 - security alerts & warnings (EWS);
 - prevention and exchange of information with other CERTs and similar organisations on national and international levels;
 - promotion and advise of local CERTs establishment.

- @ Separate CERT teams need a coordination centre and country in/out contact point.

CERT international partnership



@ RRT actively participates and collaborates within international CERT community:

- **FIRST** (Forum for Incident Response and Security Teams);
- **TERENA** (Trans-European Research and Education Networking Association);
- **NATO CERT** group on information and best practice exchange.

@ TRANSITS training workshop for CERT on 29-30 March 2006 in Vilnius was a good example of international cooperation:

- co-organized and sponsored by ENISA, TERENA and FIRST;
- CERT staff trained from numerous Europe and Asia countries;
- concentrated on operational, organizational and legal aspects of response to incidents.



In broader terms: public and private sectors partnership



@ Broad policy for trust and security requires *Public and Private Sectors Partnership*:

- Industry, science and public authorities may ensure the right balance between technology development, regulations and policy measures;
- Risk assessment, management and mainly allocation require close cooperation between technological and regulatory levels;
- The right balance between governance, policy and market dynamics should be assessed in terms of economics;
- There is a need for understanding conflicts and synergies between consumer interests (including privacy) and economics;
- Demand for technology and regulation that lead to the desired economic growth whilst providing the desired level of consumer protection.

Lithuanian public and private sectors partnership: Rising of awareness



@ In close cooperation with commerce banks 200.000 flyers with basic information about phishing threats have been distributed to users at time when growing phishing activities in Lithuania has been observed.

A flyer with a blue background and a binary code pattern at the top. The text is in Lithuanian. It includes the RRT logo, contact information for the Lithuanian Republic's Regulation of Relations Agency, and a warning to be cautious of internet data theft. A cartoon fish is shown swimming in a digital stream.

Kur kreiptis pagalbos?

Gavę „phishing“ laišką, skambinkite ir praneškite apie jį bankui, kurio darbuotoju sukčius bando apsimesti. Tai leidžia imtis tinkamų priemonių, didinant elektroninių paslaugų saugumą ir kovojant su sukčių išradingumu.

Užtikinėti kelių sukčių tyrimai – kibernetinio saugumo garantas

Jei jau suvedėte savo prisijungimo vardą, slaptažodžius, sąskaitos ar kreditinės kortelės duomenis į falsifikuotą finansinės įstaigos tinklalapį, nedelsiant skambinkite į banką ir užblokuokite prieigą prie savo sąskaitų.

Jei įtariate, kad Jūsų pinigais naudojasi elektroniniai sukčiai, kreipkitės į Nusikaltimų elektroninėje erdvėje tyrimo skyrių:
tel. (8 ~ 5) 272 53 72,
el. paštas: cyberpolice@policija.lt.

RRT

**Lietuvos Respublikos
ryšių reguliavimo tarnyba**

Algirdo g. 27, LT-03219 Vilnius
tel. (8 ~ 5) 210 56 75
faksas (8 ~ 5) 216 15 64
el. paštas cert@rt.lt

Daugiau informacijos:
<http://www.rtt.lt/phishing>

**BŪKITE ATSARGŪS:
DUOMENŲ VAGYSTĖS INTERNETE**

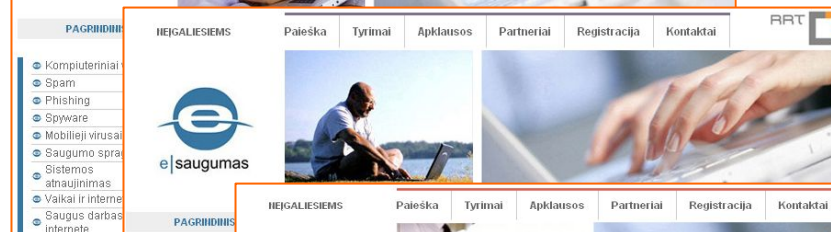
Lithuanian and private sectors partnership: Rising of awareness



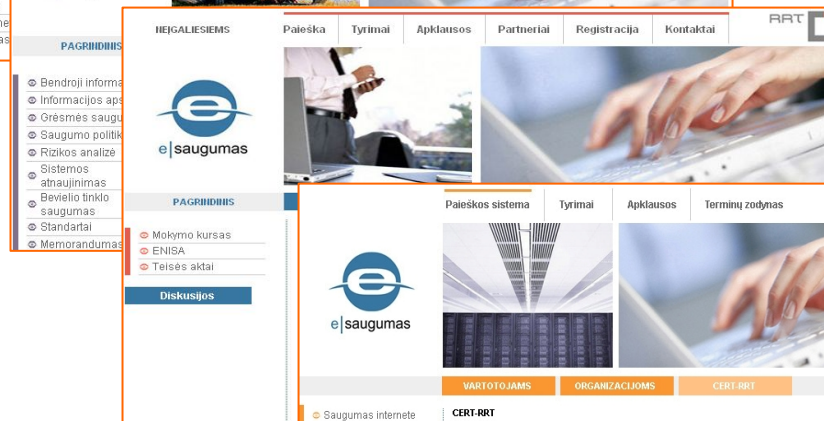
@ Interactive website www.esaugumas.lt has been created by NRA and now is being developed by numerous partners and is going to become the Internet portal of Lithuania for all interested parties which strive to provide the Internet consumers, organizations or institutions with relevant information on network and information security issues.



For home users



For enterprises



For institutions



CERT

Lithuanian and private sectors partnership: Inter-institutional cooperation



@ RRT has signed The Memorandum of Understanding on the Progress in the Area of Security of Information and Networks with the Association of Lithuanian Banks and the Association "Infobalt".

Memorandum PRIORITIES:

- I. **Investigation of information and network security incidents;**
- II. Usage of information and network security tools;
- III. Public education and training in the area of security;
- IV. Drafting of laws with the view to proper regulation of security of information and networks in the Republic of Lithuania.

Memorandum Implementation Committee, formed of the representatives of the parties, is established to take care of implementation of the Memorandum and working projects.

Lithuanian actions: Reduction of negative impact



@ RRT in cooperation with well-known security vendors work together on project “Safeguard your computer!” to produce particular tool for home users which will help to improve security on their personal computers.

- It will be realized through special CD with collection of necessary safeguard programs (*antivirus, antispam, antispyware and other*) and relevant information about secure use of Internet;
- About 100.000 CDs are planned to be issued and distributed for free;
- CD distribution action will go through Lithuanian regions in July 2006.



International partnership



@ RRT actively participates and collaborates on international level:

- **ENISA** (European Network and Information Security Agency);
- **IRG** (Independent Regulators Group) IT security working group;
- **ISACA** association;
- London action plan combating spam;
- “Spam zombies” initiative.

RRT in cooperation with ENISA and Ministry of Transport and Communications in November 2005 organized the European Network and Information Security Conference “**Readiness for advanced solutions on handling network and information security incidents**”.

Tomas Lamanaukas, RRT, Lithuania

A screenshot of the website for the European Network and Information Security Conference. The top banner features a blue background with white network lines and logos for 'AVSIJ REGULAVIMO TARNYBA', 'enisa' (European Network and Information Security Agency), and 'THE MINISTRY OF TRANSPORT AND COMMUNICATIONS OF THE REPUBLIC OF LITHUANIA'. Below the banner is a photograph of a town square with a church. A navigation menu on the left includes links for Home, Program, Venue, Travel information, Summary, and Pictures and Video. The main content area displays the conference title and dates: 'European Network and Information Security Conference', 'Readiness for Handling Network and Information Security Incidents', and 'November 24-25, 2005, in Vilnius, Lithuania'. A timestamp '2006-04-25 7:27' is visible in the top left corner of the screenshot.

Initiatives areas for international partnership



- @ Promotion of timely information exchange between CERT teams is extremely important for security incidents prevention.
 - **FIRST** (Forum for Incident Response and Security Teams);
 - **TERENA** (Trans-European Research and Education Networking Association).

- @ Botnet networks are a major reason of biggest part of incidents.
 - Latest surveys show that botnets can connect up to hundreds thousands of compromised computers; so usually it's an international problem.
 - FTC initiative "Spam zombie" is a good example and should be resumed and developed.

- @ It's necessary to promote security policy standards and security audit implementation for reaching more common worldwide security level of IT systems and products.
 - **ISACA** (Forum for Incident Response and Security Teams).

@ There's a lack of general plan and precise work program for reaching global secure information technology.

- Internet network is not adapted to high-level security requirements and needs to be replaced by new generation protocols and standards that have more security options and should be promoted their worldwide implementation :
 - **IPv6** (internet protocol);
 - **DNSsec** (Domain Name System Security Extension);
 - **SPF** (Sender Policy Framework, extension for secure e-mail system).

@ There are no contact points in some countries to deal with security issues and those white spots should be eliminated.

@ 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.

@ Wide co-operation among various public and private sectors is needed in order to create coherent network that will effect security inside the region.

@ ITU can be a body that will facilitate global actions based on the broad cooperation of various stakeholders in the IT security field.

Thank you for your attention



Tomas Lamanuskas

Deputy Director

Communications Regulatory Authority
(RRT) of the Republic of Lithuania

Address: Algirdo Str. 27, 03219 Vilnius

E-mail: tlamanuskas@rrt.lt

Telephone: +370 5 210 56 27