INTERNATIONAL CONFERENCE: CyberTerrorism and CrimeConference CYTER 2012

Place: Praha

Date: June 12 – 13, 2012

Organisation: CZECH TECHNICAL UNIVERSITY IN PRAGUE, Faculty of transport Sciences

Participants: 86 – public administration, academic sphere, private sector

Conference output: schooling of government and private sector

Programme: annex 1

Presented and published papers related to FOCUS:

JanProcházka, DanaProcházková:*KYBERNETICKÁ INFRASTRUKTURA – IDENTIFIKACE KRITICKÝCH MÍST A DOPADY JEJÍHO SELHÁNÍ (Cyber Infrastructure- identification of critical pots and impacts of its failure)*. Cyber Terrorism and Crime Conference, CYTER, ISBN 978-80-01-05072-9,CD-ROM 20p. (2012).

Abstract: In the first, article defines what Cyber infrastructure is and what part we can divide it: procedural, technical and program. Each section then has its function and its structure. Cyber infrastructure is one of the critical infrastructures on the grounds of its failure has a critical impact on the protected interests (assets). Cyber infrastructures are threatening of damage from several different sources (natural and technological disasters and the human factor intentional/unintentional). In addition, the work presented 13 methods that can be applied to assessing Cyber infrastructure and finding critical points. What-if analysis is selected of the methods and its results for the Cyber infrastructure are also presented.

AndrejPastorek:*FIRMWARE JAKO ZBRAŇ KYBERNETICKÉ VÁLKY (Firmware as a force of cyber war).* Cyber Terrorism and Crime Conference, CYTER, ISBN 978-80-01-05072-9, CD-ROM 21p. (2012).

Abstract: Paper deals with emerging role of firmware as a potential cyber warfare tool and analyses hazards associated with misuse of firmware for cyber-attacks, whether by individuals, organized groups or states. Firmware is an integral part of all ICT components; it is highly proprietary software that provides the basic functions of

the equipment.It is not available in source code, is difficult to parse, and standardization of specifications is difficult and unenforceable. Bugs in firmware always lead to substantial errors in the functionality of the equipment.Detection of potential malware code inclusion into firmware is extremely difficult. Compromised firmware can be ideal tool for industrial espionage.Unlike other forms of attacks on IT infrastructure, the attacks on firmware can completely cripple IT functionality for a long time, in some cases irreversibly.Lack of appropriate attention is a very important issue, as basically there is no overview of firmware in billions of devices that form IT infrastructure, there is no process for inspection and certification.

J. Srp, D. Procházková: *ANALÝZA KYBERNETICKÝCH SÍTÍ V SYSTÉMOVÉM POJETÍ* (Analysis of cyber networks in system concept).Cyber Terrorism and Crime Conference, CYTER, ISBN 978-80-01-05072-9, CD-ROM 22p. (2012).

Abstract: The aim of the paper is to show that all cyber networks (such as telecommunication, IT or ICT networks) are systemically identical or very similar, although each of them is applied in anotherindustry or economy field or includes other added functional elements. The effort is to show that systemic identity (similarity) of the mentioned networks identifies the same set ofnetwork security threats that can be solved using the same approaches and techniques. The integrative approach based on the systematic approach enables to effectively use the efforts of professionals and all means target to the actual problem solving. The mentioned networks classification to the cyber critical infrastructures is also made based on this concept.The paper contains examples of results "What, if" methodology concerning the cyber infrastructure failures and examples of direct and indirect impacts of such failures.

1st day of conference - Tuesday, June 12th, 2012				
11:00	12:00		Registration	
12:00	12:15		Welcoming speech	
12:15	13:00	Corvinus University of Budapest *Hungaria*	Anonymity over the internet	ZoltánBalogh
13:00	13:45	Austrian Institute of Technology *Austria*	Towards a National Cyber Attack Information System	Florian Skopik
13:45	14:30		Coffee break	
14:30	15:15	Czech Technical University in Prague *Czech Republic*	Cyber Infrastructure - Identification of Critical Spots and Impact of their Failure	Dana Procházková
15:15	16:00	Czech Technical University in Prague *Czech Republic*	Methodology for Identification of Critical Spots	Jan Procházka
16:00	16:15		Coffee break	
16:15	17:00	Czech Technical University in Prague *Czech Republic*	Anonymous and the others	VáclavJirovský
17:00	17:30		Discussion-round table	
17:30	17:45		Conclusion	

2nd day of conference - Wednesday, June 13th, 2012				
8:30	9:00		Registration	
9:00	9:45	Bull *Czech Republic*	Principles of detection of advanced cyber threats and attack	TomášDedek
9:45	10:30	Czech Technical University in Prague *Czech Republic*	Phenomenon of behavioral detection - VibraImage	Jan Tůma
10:30	10:45		Coffee break	
10:45	11:30	Czech Technical University in Prague *Czech Republic*	System analysis of cyber networks	JaroslavSrp
11:30	12:15	Czech Technical University in Prague *Czech Republic*	Firmaware as a tool of cyber war	Andrej Pastorek
12:15	13:15		Lunch	
13:15			End of the conference	