VÝZNAM „KNOWLEDGE SHARING“ V PROBLEMATIKE OCHRANY KRITICKEJ INFRAŠTRUKTÚRY

THE IMPORTANCE OF KNOWLEDGE SHARING IN PROBLEMATIC OF CRITICAL INFRASTRUCTURE

Martin HROMADA

Dostupné na http://www.population-protection.eu/attachments/042_vol4special_hromada.pdf.

Abstract

Critical infrastructure as a system is the essential part of society functional continuity, its economic or social structure and systems. In relation to this fact, there were created approaches, tools, which reflect above mentioned essentiality and created the framework for risk assessment system or that factor, which are able to affect the functionality. The article will discuss about the "knowledge sharing" aspect and its importance in problematic of critical infrastructure protection in relation to PPP (private public partnership) in context of 3rd expert meeting EU-US-CANADA.

Keywords

Critical Infrastructure, Knowledge Sharing, Functionality, Private Public Partnership.

Úvod a terminologické vymedzenie problematiky

Je potrebné konštatovať, že publikácia bude zameraná na oblasť európskej kritickej infraštruktúry a na povinnosti, ktoré vyplývajú jej prevádzkovateľom a to vo vzťahu k medzinárodnému aspektu ochrany kritickej infraštruktúry v súvislosti s knowledge sharing. Medzi základné pojmy v tejto oblasti patria:

„kritická infraštruktúra“ je zložka, systém alebo ich časť nachádzajúca sa v členských štátoch, ktorá je nevyhnutná pre zachovanie základných funkcií spoločnosti, zdravia, ochrany, bezpečnosti, kvality života obyvateľov z ekonomického a sociálneho hľadiska, a ktorej narušenie alebo zničenie by malo závažné dôsledky v členskom štáte z dôvodu nemožnosti zachovať tieto funkcie;

„európska kritická infraštruktúra“ alebo „ECI“ je kritická infraštruktúra nachádzajúca sa v členských štátoch, ktorej narušenie alebo zničenie by malo závažné dôsledky minimálne v dvoch členských štátoch. Závažnosť dôsledkov sa posudzuje podľa prierezových kritérií. Toto zahŕňa účinky vyplývajúce z medzisektorových závislostí od iných typov infraštruktúry;

„ochrana“ znamená všetky činnosti, ktorých cieľom je zaručiť funkčnosť, kontinuitu a integritu kritickej infraštruktúry s cieľom odvrátiť, zmierniť a neutralizovať hrozbu, riziko alebo zraniteľné miesto;

„vlastníci/prevádzkovatelia ECI“ sú subjekty zodpovedné za investície alebo každodennú prevádzku a investície do konkrétnej zložky, systému alebo jeho časti označené ako ECI podľa tejto smernice; [1]

„knowledge sharing“ zdieľanie znalostí je činnosť, prostredníctvom ktorej sú znalosti (tzn-. informácie, zručnosti alebo znalosti) distribuované medzi ľuďmi, priateľov alebo členov rodiny, spoločenstiev alebo organizácie, za predpokladu, že vedomosti predstavujú cenný nehmotný majetok pre vytváranie a udržiavanie konkurenčnej výhody. [2]

Zdieľanie znalostí nie je o tom dať ľuďom niečo, alebo si od nich niečo vziať, lebo to platí len pre zdieľanie informácií. K zdieľaniu vedomostí dochádza, pokiaľ sú ľudia ochotný pomôcť jeden druhému vo vývoji nových kapacít pre vybranú činnosť, čo je možné vnímať ako tvorbu procesu vzdelávania sa.[3]

Knowledge sharing v problematike ochrany kritickej infraštruktúry

Medzi významné aspekty ochrany európskych infraštruktúr (ďalej ECI) a zároveň medzi najdôležitejšie povinnosti ich prevádzkovateľov je vytvorenie určitého partnerstva (PPP – private public partnership) zo zástupcom štátu (určené ministerstvo) do ktorého gescie prevádzkovateľ patrí, vypracovanie bezpečnostného plánu prevádzkovateľa (OSP – operator security plan), kde sa identifikujú zložky prvku kritickej infraštruktúry, bezpečnostné riešenia a iné opatrenia spojené s ochranou. Vymenovanie styčného úradníka pre bezpečnosť (SLO - Security Liaison Officer), ktorý je vnímaný ako určitá komunikačná entita medzi prevádzkovateľom a štátom resp. kontaktným bodom na ochranu ECI (kontaktným bodom sa rozumie min. vnútra resp. iný zodpovedný a na koordináciu činností v rámci ochrany ECI poverený štátny orgán).

PPP – Private Public Partnership

Vytvorenia takéhoto partnerstva vytvára rámec pre efektívnu komunikáciu medzi štátnym a súkromným sektorom, teda medzi zodpovedným a štátom určeným ministerstvom a prevádzkovateľom resp. majiteľom prvku kritickej infraštruktúry. Vzhľadom na to, že v tomto vzťahu vystupuje ministerstvo ako tvorca legislatívnych, normatívny a iných nástrojov (policy maker) je vytvorenie tohto vzťahu jednou z priorít zabezpečenia spoločného prístupu a primeranej ochrany kritických infraštruktúr v rámci celého spoločenstva a nie len na národnej úrovni. Výstupom tohto partnerstva je vytvorenie komunikačného kanála ktorý umožňuje zdieľanie relevantných informácii (info sharing) a znalostí (knowledge sharing).[4]

Knowledge sharing v praxi

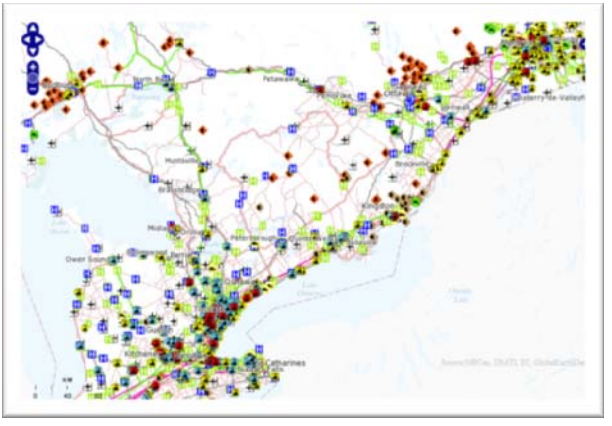
V tejto časti publikácie prezentujem praktické prístupy ku knowledge sharing, ktoré mali byť poprípade boli realizované v problematike ochrany kritickej infraštruktúry a to aj vo vzťahu k sekcii „Knowledge sharing“ (ďalej KS) na 3. Expertnom meetingu EU-US-CANADA pre oblasť ochrany kritickej infraštruktúry.

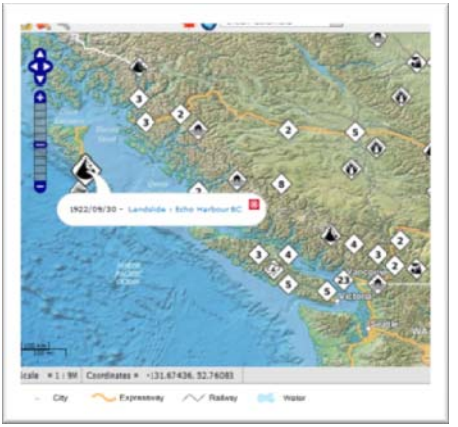
KS a CIWIN

Jednalo sa o vytvorenie internej centrálnej siete, ktorá mala umožňovať výmenu informácií medzi systémami rýchleho varovania (RAS) a príslušnými službami (ARGUS). CIWIN by mala prispieť k formovaniu priestoru pre výmenu postupov a skúseností s predmetnou problematikou a mala by fungovať ako viacúrovňový komunikační a varovní systém, kde prvá úroveň by slúžila na rýchlu výmenu varovných informácií a druhá úroveň ako fórum na výmenu myšlienok a znalostnej databázy.

KS CANADA – CI Gateway

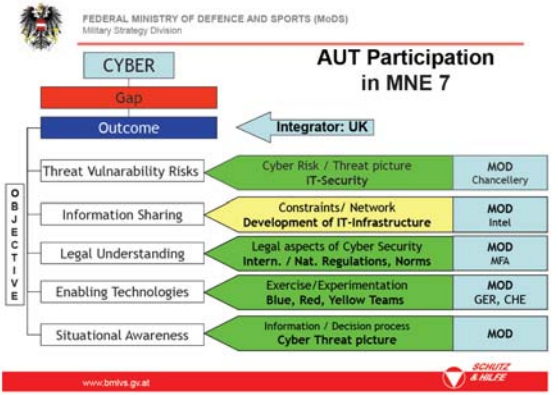
CI Gateway je šifrovaná, heslom chránená webová platforma pre zdieľanie neutajovaných informácií. Je určená pre zainteresované entity verejného a súkromného sektora v rámci vybranej siete kritickej infraštruktúry. V rámci tejto platformy dochádza k zdielaniu informácií a dokumentov k riadeniu rizík, „best practices“, hodnotiacich nástrojov či relevantných kontaktov. V rámci potreby zvyšovania situačného povedomia sú v rámci daného systému prezentované geopriestorové informácie o pohybe osôb a tovaru v prípade núdze. [5]





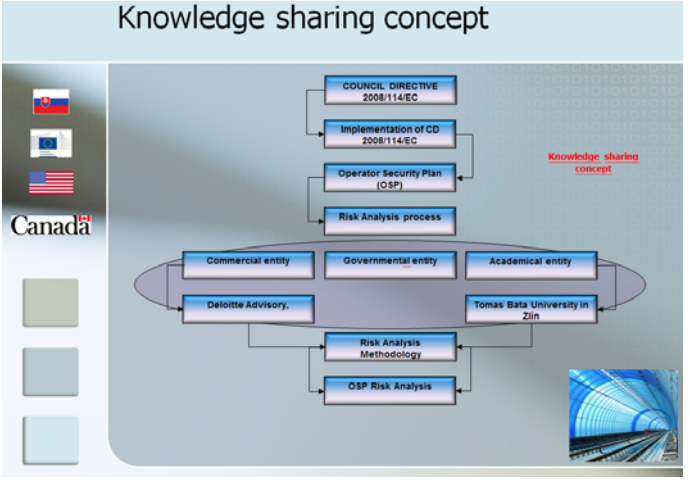
KS Rakúsko – ICT Security strategy

Potreba komplexnosti riešenia otázok ICT vznikla na základe skutočností, kde sa predpokladá, že kybernetické útoky môžu byť použité na dosiahnutie politického cieľa v čase mieru, prípravy na vojnu či v jej priebehu. Ďalej sa poukazuje na fakt, že národy s veľkou závislosťou na ICT technológiách sú často odkázané na centrálnych orgánoch, ktoré zhromažďujú, analyzujú a vyhodnocujú všetky informačné toky. Kybernetické útoky prichádzajú bez varovania a majú globálny efekt či fakt, že s využitím relatívne malých prostriedkov sa dá spôsobiť značná škoda. Tieto skutočnosti prinútili zodpovedné orgány v Rakúsku vytvoriť koncept knowledge sharing a postaviť ho na existujúcom kompetenčnom rámci v rámci ICT bezpečnosti.[6]



KS a Česká republika

Riešenie otázok ochrany kritickej infraštruktúry ČR je v súvislosti s potrebou implementácie smernice 2008/114/ES. V rámci tohto procesu vznikla povinnosť identifikácie či označenie európskych kritických infraštruktúr či ďalšie náležitosti spojené s ochranou. (vypracovanie bezpečnostného plánu prevádzkovateľa, vymenovanie styčného dôstojníka pre bezpečnosť či vytvorenie konceptu private public partnership). Nástrojom, ktorý vytvoril rámec a podporu riešenia vzniknutých povinností je v ČR bezpečnostný výskum na ktorý sa odvoláva aj „Komplexní strategie ČR k řešení problematiky kritické infrastruktury“[7]. Tento aspekt podporil vytvorenie konceptu knowledge sharing a to v procese tvorby bezpečnostných plánov prevádzkovateľa európskej kritickej infraštruktúry či plánov krízovej pripravenosti subjektu kritickej infraštruktúry.



Záver

Publikácia diskutovala o postavení a význame knowledge sharing v oblasti riešenia bezpečnostných otázok so zameraním na kritickú infraštruktúru a private public partnership ako významný aspekt jej ochrany. Nasledujúca časť textu pojednávala o praktických prístupoch využitia knowledge sharing v problematike ochrany kritickej infraštruktúry prezentovaných na 3. Expertnom meetingu EU-US-CANADA v problematike ochrany kritickej infraštruktúry konaného v Bruseli, kde boli prezentované vybrané niektoré zahraničné prístupy či naplnenie tejto filozofie z pohľadu ČR.

Za podpory Ministerstva vnútra ČR v rámci výskumného projektu č. VG20112014067 a súčasne Európskeho fondu regionálneho rozvoja v rámci projektu CEBIA-Tech č. CZ.1.05/2.1.00/03.0089.

Literatúra

[1] Smernica rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu. Dostupné na WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:SK:PDF>.

[2] MILLER, D., SHAMSIE, J. "The resource-based view of the firm in two environments: The Hollywood film studios from 1936 to 1965". *Academy of Management Journal*, 1996, Vol. 39, No. 3) 39 (3): 519–543.

[3] SENGE, P. *Knowledge Sharing,* Knowledge sharing, David Gurteen web page. Dostupné na WWW: <http://www.gurteen.com/gurteen/gurteen.nsf/id/knowledge-sharing>.

[4] HROMADA, M. Povinnosti prevádzkovateľa Európskej kritickej infraštruktúry/The European Critical Infrastructure Operator Duties. *Security Magazín*, 2010, č. 95. ISSN 1210-8723.

[5] ELLINGTON, S. Canadian Knowledge Sharing Practices: Canadian Critical Infrastructure Information Gateway and the Movement of People and Goods in the Event of an Emergency, Public Safety Canada. *3rd EU-US-Canada Expert Meeting on Critical Infrastructure Protection (CIP)*, Brussels, May 22nd-23rd 2012.

[6] SCHROEFL, J. Sharing risk analysisi across borders and sectors – view from a national perspective. *3rd EU-US-Canada Expert Meeting on Critical Infrastructure Protection (CIP)*, Brussels, May 22nd-23rd 2012.

[7] Výbor pro civilní nouzové plánování. Komplexní strategie České republiky k řešení problematiky kritické infrastruktury. 2009.

[8] HROMADA, M. Knowledge sharing in the risk analysis process in the energy sector. *3rd EU-US-Canada Expert Meeting on Critical Infrastructure Protection (CIP)*, Brussels, May 22nd-23rd 2012.

Kontaktní údaje:
Ing. Martin Hromada, Ph.D.,
Ústav bezpečnostního inženýrství, Fakulta Aplikované informatiky, Univerzita Tomáše Bati ve Zlíně, Nad Stráněmi 4511, 760 05 Zlín,
e-mail: hromada@fai.utb.cz, tel.: +420 57 603 5243.