MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 3
KONCEPCE KYBERNETICKÉ OBRANY V EU A OSTATNÍCH ZEMÍCH (V ARMÁDÁCH NATO)

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

Operační program Vzdělávání pro konkurenceschopnost

Projekt: ***Vzdělávání pro bezpečnostní systém státu***

(reg. č.: CZ.1.01/2.2.00/15.0070)

esf evropský sociální fond v ČR | EVROPSKÁ UNIE | MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY | OP Vzdělávání pro konkurenceschopnost | UNIVERZITA OBRANY

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Kybernetická bezpečnost

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby. Lisabonský summit NATO uskutečněný v roce 2010 mimo jiné zdůraznil nutnost řešení této problematiky jak na mezinárodní úrovni, tak i na úrovni národní. Bezhraničnost a všudypřítomnost kybernetických hrozeb vyžaduje intenzivní mezinárodní spolupráci a také intenzivní úsilí při zajišťování kybernetické bezpečnosti jednotlivých států.

Vznikem sociálních sítí, herních sítí a zájmových sítí se z nejznámější části kyberprostoru, z internetu, stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat.

Kybernetická bezpečnost v EU a v USA

Belgie

Dánsko

Litva

Německo

Nizozemsko

Norsko

Rakousko

Slovensko

Spojené království

Španělsko

Spojené státy americké (USA)

Maďarsko

Estonsko

Polsko

Kybernetická bezpečnost v Belgii

Služby národního CERT v Belgii zajišťuje tým CERT.be, který je provozován belgickou Sítí národního výzkumu BELNET, které tuto odpovědnost předala Federální veřejná služba pro informační a komunikační technologie ve spolupráci s Belgickým institutem pro poštovní služby a telekomunikace. Jedná se o veřejnou službu, jejímž posláním je poskytování informací a koordinačních služeb za účelem zajištění informační bezpečnosti. Tyto služby jsou poskytovány nejen státním orgánům a provozovatelům kritické infrastruktury, ale také soukromým subjektům a široké veřejnosti. https://www.cert.be

Kybernetická bezpečnost v Dánsku

V Dánsku figuruje tým pod názvem DK.CERT, který je vnímán jako národní na základě toho, že jde o jednoho z průkopníků. Založen byl již v roce 1991 podle vzoru amerických CERTů dánským Centrem informačních technologií pro vývoj a výzkum, jež je národní organizací spadající pod dánské Ministerstvo školství. Hlavním cílem tohoto týmu je získávání know-how a informací prostřednictvím spolupráce s FIRST.

V Dánsku dále působí „Danish GovCERT“, který se označuje za „National“. Je provozován Ministerstvem obrany a je členem skupiny týmů s ověřeným vládním/národním mandátem při CERT/CC.

Kybernetická bezpečnost v Litvě

Kybernetická bezpečnost je v gesci Ministerstva vnitra, které koordinuje aktivity všech zainteresovaných orgánů státní správy.

V poslední době v Litvě vznikl dokument Program rozvoje bezpečnosti elektronické informace (kybernetické bezpečnosti) na období 2011 - 2019. Ten se zaměřuje především na nebezpečné internetové fenomény, které ohrožují nejen soukromé uživatele, ale i státní správu.

Kybernetická bezpečnost v Německu

Problematikou kybernetické bezpečnosti se v Německu zabývá Strategie pro kybernetickou bezpečnost, která je postavena na činnosti dvou základních orgánů. Prvním z nich je Centrum pro kybernetickou obranu, které podléhá Spolkovému úřadu pro informační bezpečnost.

Druhým zmíněným orgánem je Rada kybernetické bezpečnosti, která by měla začít pracovat 1. dubna 2012. Rada bude součástí Kancléřství a jejími členy budou nejvyšší představitelé všech relevantních ministerstev.

https://www.bsi.bund.de/

Kybernetická bezpečnost v Nizozemí

V Nizozemsku funguje tým NCSC-NL, jehož fungování v Nizozemsku zajišťuje Ministerstvo bezpečnosti a spravedlnosti, který provozuje službu pro zajištění kybernetické bezpečnosti Nizozemska a vystupuje jako Incident response team pro vládu Nizozemska. Pracuje zejména pro organizace zajišťující veřejné služby, typicky vládní organizace, a spolupracuje se subjekty, které jsou aktivní v rámci kritické infrastruktury Nizozemska. NCSC-NL také spolupracuje s mezinárodní sítí pracovišť typu CERT . http://www.govcert.nl

Kybernetická bezpečnost v Norsku

Vojenský i národní CERT jsou v podřízenosti Národního bezpečnostního úřadu. Národní CERT v Norsku vystupuje pod zkratkou NorCERT, a koordinuje preventivní činnosti v rámci zabezpečení informační a komunikační infrastruktury Norska. Má za úkol také koordinaci protiopatření pro případ bezpečnostních incidentů a ochranu kritické infrastruktury Norska. NorCERT vznikl v roce 2006 a je operačním oddělením Národního bezpečnostního úřadu Norska, které se skládá z dvou integrovaných sekcí – Norský systém pro upozornění a brzké varování systémů digitální infrastruktury, a Sekce pro Incident Handling, jež je národním centrem. https://www.nsm.stat.no

Kybernetická bezpečnost v Rakousku

V Rakousku figuruje národní CERT tým pod názvem CERT.at, který vznikl z iniciativy rakouského doménového registrátora nic.at. Vystupuje jako point of contact pro kybernetickou bezpečnost v národním kontextu, také koordinuje ostatní CERT týmy působící jak v rámci kritické infrastruktury Rakouska, tak i v rámci ostatních rakouských sítí. Mimo jiné má CERT.at za úkol informovat veřejnost o bezpečnostních rizicích a incidentech. http://www.cert.at.

Kybernetická bezpečnost na Slovensku

Národní CERT tým vystupuje pod názvem CSIRT.SK, který vznikl v roce 2009 v souladu s Národní strategií pro informační bezpečnost ve Slovenské republice z roku 2008. CSIRT.SK je zřízený jako specializovaný útvar DataCentra, které je rozpočtovou organizací Ministerstva financí SR. Tento tým má zejména iniciovat a koordinovat reakce státní správy, veřejného a soukromého sektoru na bezpečnostní incidenty, které ohrožují nejen Národní informační a komunikační infrastrukturu SR (NIKI). Computer incident response team Slovakia vznikl usnesením vlády Slovenské republiky č. 479/2009 ze dne 1. června 2009, viz http://www.csirt.gov.sk/.

Kybernetická bezpečnost v Británii

Britské ministerstvo vnitra nedávno zveřejnilo novou národní Strategii kybernetické bezpečnosti do roku 2015, ve které vymezuje základní cíle pro ochranu kybernetického prostoru a postupy, kterými jich chce dosáhnout. Primárně se politika kybernetické bezpečnosti UK zaměřuje na ochranu proti kyberterorismu.

Důležitá je pochopitelné také ochrana kritické infrastruktury.

V neposlední řadě je cílem ochrany také bezpečný internet.

Ve Spojeném království byl v roce 2008 ustaven GovCertUK, který je vládním týmem a jeho hlavním úkolem je pomáhat veřejnému sektoru při řešení bezpečnostních incidentů.

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Kybernetická bezpečnost ve Španělsku

Jejím zajištěním jsou pověřeny tři základní instituce. Tou hlavní je Národní kryptologické centrum (CCN), které patří pod Ministerstvo obrany a je součástí Národního zpravodajského centra. Tato agentura je zodpovědná za koordinační činnost jednotlivých státních orgánů, které používají šifrovací prostředky a postupy. Jejím hlavním cílem je zajistit bezpečnost informačních technologií, které jsou v tomto prostředí využívány. CCN je také členem Vysoké rady pro elektronickou správu a Národního centra pro ochranu kritické infrastruktury.

Kybernetická bezpečnost v Maďarsku

CERT- Hungary je vládní Reakční tým pro počítačové incidenty (CSIRT), je vládním CERT týmem Maďarska. Funguje v rámci nadace Theodora Puskáse. CERT Maďarsko zahájil svoji činnost v lednu 2005. Od ledna 2010 CERT Maďarsko funguje, na základě vládního rozhodnutí, jako Centrum kybernetické bezpečnosti Maďarska. CERT Maďarsko koordinuje preventivní aktivity a odpovědi na porušení IT bezpečnosti zaměřené na kritickou infrastrukturu Maďarska. Nad činností CERT Maďarska dohlíží Úřad předsedy vlády.

Za účelem zajištění efektivní odpovědi proti kybernetickým hrozbám CERT Maďarsko aktivně spolupracuje s národními partnery, podílí se na snahách mezinárodních CSIRT a CIIP organizacích.

Kybernetická bezpečnost v Estonsku

Estonsko nemá speciální právní úpravu problematiky kybernetické bezpečnosti, ale vychází ze Strategie v oblasti kybernetické bezpečnosti. Původně bylo gestorem v oblasti kybernetické bezpečnosti ministerstvo obrany, nyní má tuto problematiku na starosti ministerstvo hospodářství a dopravy, do jehož působnosti spadají komunikace.

V Estonsku mj. jako reakcí na kybernetický útok v roce 2007, bylo zřízeno NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Toto Centrum bylo založeno v květnu 2008 a v říjnu téhož roku bylo akreditováno jako NATO Centre of Excellence a má statut mezinárodní vojenské organizace, není však operační jednotkou ani součástí velitelské struktury NATO.

Kybernetická bezpečnost v Polsku

Vládní tým pro řešení kybernetických incidentů v Polsku je CERT.GOV.PL

Poskytuje technickou podporu pro zajištění a rozvíjení ochrany státní správy a samosprávy Polské republiky před kybernetickými hrozbami. Působí v rámci oddělení teleinformatické bezpečnosti kontrarozvědné služby ABW.

Kybernetickou bezpečnost v Polské republice formálně upravuje vládní program ochrany kyberprostoru Polské republiky v letech 2009 až 2011. Na něj navazuje program na léta 2011 až 2016, který by měl být v krátké době vládou schválen.

Kybernetická bezpečnost v USA

V širší podobě je toto téma definováno ve strategických dokumentech, tj. prezidentově *Cyberspace Policy Review (2009)*, *Národně bezpečnostní strategii* (NSS z roku 2010) a O*branné doktríně* (QDR z roku 2010). Do oblasti kybernetické bezpečnosti je zapojeno několik agentur a ministerstev.

V květnu 2011 administrativa zveřejnila klíčovou *International Strategy for Cyberspace.*

Ministerstvo obrany povýšilo kybernetický prostor na svou pátou válečnou doménu vedle souše, vzduchu, moře a vesmíru.

Závěr

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby. Lisabonský summit NATO uskutečněný v roce 2010 mimo jiné zdůraznil nutnost řešení této problematiky jak na mezinárodní úrovni, tak i na úrovni národní. Bezhraničnost a všudypřítomnost kybernetických hrozeb vyžaduje intenzivní mezinárodní spolupráci a také intenzivní úsilí při zajišťování kybernetické bezpečnosti jednotlivých států.

Vznikem sociálních sítí, herních sítí a zájmových sítí se z nejznámější části kyberprostoru, z internetu, stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat.

Dotazy?

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ