Received: 15. 6. 2019 Accepted: 15. 6. 2019 Published on-line: 15. 6. 2019
Available from: www.obranaastrategie.cz doi: 10.3849/1802-7199.19.2019.01.055-056

PAČKA, Roman. CSIRT: V přední linii boje proti kybernetickým hrozbám. Brno: CDK, 2019. Politologická řada, 590. ISBN 978-80-7325-473-5.

Jakub Fučík[a]

V letošním roce vydalo nakladatelství CDK knihu *CSIRT: v přední linii boje proti kybernetickým hrozbám* (132 s.), jejímž autorem je Roman Pačka. Obecně se publikace zaměřuje na tzv. Computer Security Incident Response Team (CSIRT/CERT) a jejich roli při zajišťovány kybernetické bezpečnosti. Cílem je prozkoumat jejich význam pro národní bezpečnost a identifikovat jejich pozici v bezpečnostním systému státu ve vztahu k ostatním bezpečnostním složkám státu a výzvám, kterým čelí. Autor se tak zabývá velmi aktuálním a minimálně v domácím prostředí téměř nezpracovaným tématem. Na druhou stranu, v kontextu narůstající důležitosti kyberprostoru a potřebného zajišťování národních (bezpečnostních) zájmů v něm bude přínos dotčeného výzkumu jen posilovat. Právě na tento trend je poukázáno i v první, teoretické části publikace. Kybernetická bezpečnost je zde vhodně zarámována skrze přístup tzv. Kodaňské školy (kap. 1.1), a to zejména se zohledněním přesahů do jednotlivých sektorů a diskuzí procesu sekuritizace.

Kromě úvodu a závěru je publikace rozdělena do čtyř hlavních kapitol. První kapitola (Kybernetická bezpečnost) slouží, jak již bylo uvedeno výše, jako teoretické vymezení a zdůvodnění poslání a činnosti jednotlivých aktérů při zajišťování bezpečnosti v oblasti kyberprostoru. Konkrétně tato část poskytuje základní východiska pro interpretaci významu CSIRTů a čtenáři předkládá potřebné uvedení do zkoumané problematiky. Následuje kapitola „Computer Security Response Team - CSIRT“, která se zaměřuje na vydefinování charakteru tohoto aktéra. Jeho uchopení v textu lze jednoznačně považovat za komplexní.

Od základního vymezení (kap. 2.1) přechází autor k roli jednotlivých týmů. Jejich úlohu charakterizuje prostřednictvím tří základních kritérií – poslání CSIRTu, jeho působnost (tzv. „constituency“) a organizační zakotvení. Posléze je ukázána návaznost těchto kritérií na typologii dotčených aktérů. Autor shrnuje jednotlivé kategorie prostřednictvím velmi přehledných tabulek. Současně se z ohledem na zajišťování národní bezpečnosti podrobněji zaměřuje na vybrané subjekty, jak na mezinárodní (kap. 2.3.2), tak vnitrostátní úrovni (kap. 2.3.1). Působnost CSIRTů je dále doplněna pojednáním o poskytovaných službách (kap. 2.4) a vztazích napříč jednotlivými pracovišti a bezpečnostní komunitou jako celkem (kap. 2.5).

Druhou kapitolu doplňuje historický vývoj těchto aktérů jak v zahraničí (kap. 2.6), tak na domácí scéně (2.6.1). Právě tato oblast je následně podrobněji prozkoumána

[a] Centre for Security and Military Strategic Studies, University of Defence in Brno. Brno, Czech Republic. jakub.fucik@unob.cz. G-8537-2013.

prostřednictvím případové studie českého národního CSIRTu *GovCERT.cz*. Zvolený případ čtenáři velmi dobře ilustruje a propojuje informace z předchozích podkapitol, čímž napomáhá logickému přechodu na další zkoumanou oblast.

Touto oblastí (kap. 3) je vymezení postavení CSIRTů v bezpečnostním systému a jejich vztahů s ostatními bezpečnostními složkami. Obecně je toto téma rozděleno do dvou hlavních částí – interakce s policií a zpravodajskými službami (kap. 3.1) a interakce s ozbrojenými silami (kap. 3.2) – což mj. reflektuje i specifické požadavky na zajišťování vnitřní a vnější bezpečnosti, přičemž např. právě v působení zpravodajských služeb dochází k určitému prolínání. Spolupráce s policií a zpravodajskými službami je především rámována konceptem kybernetické bezpečnosti. Autor nejprve poukazuje na specifické aspekty dotčených složek při jejím zajišťováním. Příkladem je působení zpravodajských složek a jejich dalších cílů v oblasti národní bezpečnosti, které mohou být naplňovány úmyslným ponecháním identifikované zranitelnosti informačních systémů a jejího využívání pro vlastní operace. Právě zde vzniká potenciální kolize se zájmy/cíli policie nebo samotných CSIRTů na straně druhé, které v duchu zajištění bezpečnosti informačních systémů směřují, pokud možno, k co nejrychlejšímu a nejefektivnějšímu odstranění identifikovaného problému (srov. kap. 3.1.1 a 3.1.2). Následně je podrobně diskutována samotná spolupráce mezi těmito aktéry. V textu nechybí jak identifikace potenciálních úskalí a doporučení k jejich překlenutí, tak výhod a příležitostí, které z nastavených vazeb vyplývají (kap. 3.1.3 a 3.1.4).

Oproti tomuto vymezení jsou interakce s ozbrojenými silami rámovány zejména prostřednictvím konceptu kybernetické obrany, byť dochází k jejímu úzkému propojování právě s kybernetickou bezpečností (kap. 3.2). Současně z pohledu rapidního vývoje v této oblasti na jedné straně a relativně nového fenoménu ve válečnictví (např. i ve vztahu k mezinárodnímu právu) na straně druhé, přináší tato část velmi důležité podněty do diskuze o tomto tématu. Příkladem je možné nastavení systému národní spolupráce nebo odlišování jednotlivých typů síťových operací.

Závěrečná – čtvrtá – kapitola analyzuje výzvy, které (kromě již uvedeného) ovlivňují zajišťování bezpečnoti ze strany diskutovaných pracovišť a v případě nevhodného adresování mohou negativně ovlivnit efektivitu/úspěšnost těchto aktérů. Především je diskutována problematika sdílení informací, důvěry napříč dotčenou komunitou, komercionalizace kybernetické bezpečnosti, politizace jednotlivých aspektů a otázka personálního zabezpečení (kap. 4.1–4.5). Zpracování každého z těchto témat se vyznačuje logickou návazností a podrobnou argumentací, což jednoznačně podporuje závěry, které z nich vyplývají.

Roman Pačka svojí publikací poskytuje zajímavý pohled na existenci a fungování CSIRTů a jejich významu pro (národní) bezpečnosti. Vymezené cíle publikace byly jednoznačně splněny a text přináší důležité informace, myšlenky a podněty do debaty o kybernetické bezpečnosti/obraně. Klíčovým poznatkem na závěr jsou mj. i autorova zjištění o postupné vývoji charakteru CSIRTů, a to v posunu zejména od oblasti ryze technického řešení incidentů do mnohem širšího a politicky provázaného zajišťování národní bezpečnosti. Právě s tímto procesem jsou spojeny nové výzvy a příležitosti jak pro stávající bezpečnostní systém, tak pro příslušné CSIRTy.