Kód tématu: 026-IT-CZ

Digitální forenzní technologie při řešení útoků v kyberprostoru

Školitel: prof. Mgr. Jašek Roman, Ph.D., DBA

Konzultant: Ing. Malaník David, Ph.D., ---

Ústav fakulty: Ústav informatiky a umělé inteligence

Studijní program: Informační technologie

Anotace:

Kybernetické útoky proti IT infrastruktuře vykazují dlouhodobě vzestupný trend a jsou pro společnost i průmyslové podniky kritické. Jedná se o útoky, které jsou pro útočníky velmi lukrativní a v současné době jim poskytují i vysokou míru anonymity. Dále se ukazuje, že zvláště APT útoky jsou schopné překonávat mnoho ochranných prvků. Pokud jsou útočníkem tyto prvky překonány, poskytnou mu mnohdy neomezený přístup do celé infrastruktury sítě. Toto je zvlášť nebezpečné v současnosti, kdy jsou do sítě integrovány prvky Internetu věcí a obecně SMART technologií. Úspěšný útok může způsobit obrovské škody nejen technologické, ale i společenské. V případě zaznamenání útoku, je nutné provést jeho analýzu s využitím digitálních forenzních technologií, které mohou dát odpověď na otázky vstupního bodu útoku a také mohou poukázat na slabá místa/zranitelnosti díky kterým bylo možné útok realizovat. Cílem disertační práce je výzkum digitálních forenzních technologií použitelných pro analýzy zachycených útoků proti IT infrastruktuře. Dále se bude práce zabývat stanovením oblastí, ve kterých jsou současné forenzní technologie neúčinné. Výstupy práce by měly směřovat k návrhu systémů, či strategií využití forenzních digitálních technologií při analýze a předcházení hrozeb typu APT.

Literatura:

[1] BARRETT, Diane M. a Gregory KIPPER, LILES, Samuel (ed.). Virtualization and forensics: a digital forensic investigator's guide to virtual environments. Amsterdam: Elsevier, 2010. ISBN 978-1-59749-557-8.

[2] PORADA, Viktor a Marián SVETLÍK (eds.). Digital Forensic Forum Prague 2007: specialized digital forensic forum & meeting : proceeding of the conference. Karlovy Vary: Vysoká škola Karlovy Vary, 2008. ISBN 978-80-254-1536-8.

[3] CARBONE, Fernando a Eleanor Leonne BENNETT. Computer forensics with FTK: enhance your computer forensics knowledge through illustrations, tips, tricks, and practical real-world scenarios. Birmingham, England: Packt Publishing, 2014. Community experience distilled.

[4] ORZACH, Yoram. Network analysis using Wireshark cookbook. Birmingham: Packt Publishing, 2013. ISBN 978-1-84951-765-2.

[5] KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. První vydání. Praha: Grada Publishing, a.s., 2015, 183 stran. ISBN 978-80-247-5453-6.

[6] SINGER, P. Cybersecurity and cyberwar: what everyone needs to know. Oxford: Oxford University Press, 2014, viii, 306 s. ISBN 978-0-19-991811-9.

[7] GLENNY, Misha. Temný trh: kyberzloději, kyberpolicisté a vy. 1. vyd. v českém jazyce. Praha: Argo, 2013, 270 s. ISBN 978-80-7363-522-0.

[8] KOSTOPOULOS, George K. Cyberspace and cybersecurity. Boca Raton: CRC Press, 2013, xvii, 218 s. ISBN 978-1-4665-0133-1. Dostupné také z: http://www.loc.gov/catdir/enhancements/fy1303/2012288209-b.html.

[9] VACCA, John R. Computer and information security handbook. 2nd ed. Waltham, MA: Elsevier/Morgan Kaufmann, 2013, xxviii, 1171 s. ISBN 978-0-12-394397-2.