Posudek vedoucího diplomové práce

Název práce: Správa hrozeb pro CERT/CSIRT týmy
Autor: Jiří Machálek

Předkládaná diplomová práce vychází z potřeb řešení bezpečnostních incidentů z oblasti domén a fungování systému DNS, a to s ohledem na potřeby týmů CERT (Computer Emergency Response Team), resp. CSIRT (Computer Security Incident Response Team). Přesněji s ohledem na potřeby spíše menších týmů CERT/CSIRT, které nemají diferencované potřeby pro jednotlivé členy týmu.

Autor práce nejprve (ve své druhé kapitole) analyzuje potřeby takovýchto týmů při řešení obvyklých incidentů, nejprve v širším kontextu a posléze i specificky z pohledu bezpečnostního týmu CZ.NIC-CSIRT, který provozuje sdružení CZ.NIC. Následně (ve třetí kapitole) rozebírá již existující podpůrné nástroje, využitelné pro řešení incidentů, pro jejich evidenci a vyhodnocování.

Těžištěm práce pak je návrh vlastního nástroje pro správu hrozeb týkajících se domén, který je řešen jako webová aplikace charakteru nadstavby nad existujícími a již provozovanými systémy správy požadavků (konkrétně systému Request Tracker), s možností čerpat data z celé řady dostupných zdrojů, včetně těch neveřejných. Nejprve je v práci (v kapitole 4) rozebrána koncepce zvoleného řešení (nástroje Malicious Domain Manager, MDM), a posléze (v kapitole 5) popsána i jeho implementace.

Výsledkem je prakticky použitelný nástroj, který je nasazen již od druhé poloviny roku 2011 ve sdružení CZ.NIC, nejprve v testovacím provozu. Ten byl zakončen veřejným představením nástroje MDM na 35. setkání pracovní skupiny TF-CSIRT koncem ledna 2012 v Římě, a vydáním nástroje MDM pod licencí GNU GPL pro volné použití dalšími CERT/CSIRT týmy.

Výsledný nástroj Malicious Domain Manager je dnes rutinně používán týmem CZ.NIC-CSIRT, který je s jeho fungováním velmi spokojen. To, jak nasazení MDM pomáhá řešení incidentů spojených s doménami, dokládají i grafy, prezentované v samotné práci (v kapitole 6, s výsledky praktického nasazení).

Závěrem rád konstatuji, že autor prokázal velmi dobrou znalost problematiky práce CERT/CSIRT týmů a jejich potřeb, stejně jako problematiky řešení bezpečnostních incidentů, a vytvořil prakticky použitelný (a skutečně používaný) nástroj, který dovedl až do podoby verze, uvolněné pod GPL licencí. Na zadaném úkolu přitom pracoval samostatně a dokázal jej plně zvládnout.

Předkládaná práce splňuje všechny požadavky, kladené na diplomovou práci, a doporučuji připustit ji k obhajobě.

V Praze, dne 11.5.2012