Posudek oponenta k diplomové práci

předložené na Matematicko-fyzikální fakultě
Univerzity Karlovy v Praze

Autor/ka: Bc. Jiří Machálek

Název práce: Správa hrozeb pro CERT/CSIRT týmy

Studijní program a obor: teoretická informatika

Rok odevzdání: 2012

Jméno oponenta: Dan Lukeš

Pracoviště: SISAL MFF UK

V práci samé je deklarován cíl takto:

V této práci chci seznámit čtenáře s problematikou činnosti týmů CERT/CSIRT a analyzovat jejich potřeby při řešení hrozeb a problémů spojených se systémem Domain Name System (DNS) a jeho doménami. Současně chci zpracovat základní přehled podpůrných nástrojů pro práci CERT/CSIRT týmů při řešení problémů s doménami, navrhnout koncepci vlastního nástroje a implementovat jej.

Naneštěstí, otázka přesné interpretace cílů vytváří ostrou hranici mezi prací kvalitní, která stanovených cílů dosáhla, a prací který se s zadáním nevypořádala v dostatečné míře.

V teoretické části práce autor zmiňuje především ty potřeby CERT-CSIRT týmů, které jsou triviálně zřejmé ze samotné základní náplně činnosti a smyslu existence těchto skupin. Při detailnější analýze ale čerpal z informací od pouhých dvou týmů, které pocházejí ze podobného prostředí a navíc mají společné kořeny. Autor se nepokusil zjistit, zda společné cíle nevedou v reálném světě k používání jen několika málo pracovních postupů jimiž teamy těchto cílů dosahují. Tím pádem ani detailnější nezjišťoval zda existují nějaké obvyklé či převažující potřeby, které by bylo vhodné řešit v obecně použitelném podpůrném nástroji. Tím, že při podrobném zkoumání analyzoval potřeby jen jednoho typu týmu (a vlastně jen jediného týmu) mohl zcela minout možné potřeby týmů působících v odlišném prostředí - třeba týmy podnikové, u kterých lze očekávat poněkud jiný styl fungování a z toho plynoucí odlišné potřeby. Mohl minout i potřeby týmů stejného typu, pokud by existovalo víc podstatně různých postupů, kterými lze incidenty řešit. Což nezkoumal.

Ambivalentní vztah pak mám o praktické části práce, konkrétnímu programu určeném pro podporu práce CZ.NIC-CSIRT. Program je velmi přesně "ušit na míru" právě tomuto konkrétnímu týmu, jeho současným pracovním postupům v té podobě v jaké je současní zaměstnanci týmu používají. V tomto ohledu jde o excelentní dílo, ukázku velmi dobré analýzy potřeb zcela konkrétního prostředí a jejich následná dobrá implementace.

To je ale současně velkou vadou této konkrétní implementace. Program není příliš vhodný pro podporu týmů s jen trochu jiným pracovním postupem. Dokonce i změna pracovních postupů v rámci tohoto jediného týmu by mohla znamenat velký problém. Program například postrádá mechanismy, které by umožňovaly vyřizování agendy dvěma operátory současně. Nic nebrání tomu, aby jeden incident začali obvyklým postupem vyřizovat oba operátoři paralelně. To při

počtu incidentů, které CZ.NIC tým řeší není problém s ohledem na to, že oba sedí ve stejné místnosti a snadno se "dohodnou". Ale nefungovalo by to, pokud by měli operátoři pracovat například z domova či jinak prostorově vzdálených míst. Program nezná ani koncept „můj incident", který by umožnil jednomu operátorovy zobrazit (nebo i jen zvýraznit) incidenty, jejichž řešení zahájil právě on tak, aby mohl v jejich řešení pokračovat. To program diskvalifikuje pro prostředí, kde se má s ohledem na klienta za výhodné aby jeden problém řešil pokud možno jeden operátor, ten, který ho řešit začal.

Chybí i systém práv – aktuální implementace zná pouze dvě "úrovně", tedy uživatel, který smí "všechno" až na zakládání dalších uživatelů – a uživatel, který může opravdu všechno. To postačuje v prostředí týmu CZ.NIC, mám ale pochybnosti, že by to postačovalo v prostředí některého podnikového týmu, kde lze očekávat, že bude nutná nejméně jedna další úroveň, a to právo "prohlížet bez modifikací". Nakonec, takové právo by nejspíš ocenil i tým CZ.NICu. až bude poprvé docházet k personální změně a bude nutné zaučit nového zaměstnance. Týmy fungující méně neformálně nebo ty s velmi velkým počtem řešených incidentů by pak mohly postrádat systém eskalací, který by umožnil mít operátory více úrovní (méně kvalifikované operátory pro řešení méně náročných problémů, které tvoří většinu případů a vedle nich menší počet kvalifikovanějších operátorů pro méně obvyklé incidenty)

Všechny zmíněné vady, jak teoretické tak praktické části práce jsou ale ve skutečnosti vadou jedinou – práci zcela chybí "střed", který by propojoval všeobecné konstatování potřeb víceméně zjevně plynoucí ze samotné definice účelu existence skupin tohoto typu a na druhé straně konkrétní implementace které se opírala o potřeby zcela konkrétního týmu. Nepřítomnost této části neumožnila autorovi mít potřebný nadhled, který je potřeba pro implementaci takových funkcí, které sice právě teď a právě pro tento tým třeba nejsou, jejichž užitečnost ale lze rozumně předpokládat pro jiný tým, nebo i pro případ změn v systému práce týmu zkoumaného.

Za ocenění stojí dokumentace MDM, která je dobrá a významně by usnadnila úpravy či doplnění chybějících funkcí programu. A příprava na snadnou lokalizaci programu do jiných jazyků pak ukazuje, že autor přeci jen na možnou existenci jiných týmů zcela nezapomněl.

Nakonec to je ale především velmi dobrá analýza aktuálních potřeb zcela konkrétního zadavatele a následná kvalitní implementace řešení, která mě přesvědčila, že přes všechny výhrady by práce měla být obhájena. Nicméně, kvůli nedostatkům teoretické části a zejména malém vzorku (a nereprezentativnímu výběru) týmů jejichž potřeby autor zkoumal, považuji za odpovídající známku „3".

Datum: 14. května 2012

Podpis: 

Dan Lukeš