Autor: Ladislav Hanzlíček
Školitel: Prof. Ing. Petr Doucek, CSc.

Disertační práce – Prezentace pro oborou radu – abstrakt

Téma: Prioritization of vulnerability remediation using laws of vulnerabilities and threat intelligence

Problémová oblast

Díky své profesi jsem měl možnost účastnit se několika projektů, které se týkaly zavádění procesů a systému pro řízení zranitelností a ze zkušenosti mohu říci, že pro zákaznickou organizaci jsou to obtížné projekty.

Nelehkou úlohou, které organizace čelí je zejména vyrovnat se s obvykle vysokým počtem kritických zranitelností a potýkají se s problémem, jak stanovit strategie pro odstraňování zranitelností (včetně přijímání případných kompenzačních opatření).

Cíle výzkumné činnosti

Navrhované zaměření výzkumné činnosti cílí na zranitelnosti ICT a lepší pochopení, jaké jsou zákonitosti zranitelností v reálném světě. Toto s vědomím, že odhalování zranitelností a jejich řešení je důležitou vrstvou v konceptu bezpečnosti „defence in depth“.

Cíle pro výzkumnou činnost jsou následující:

I. Cílem práce je navrhnout metodiku prioritizace odstraňování zranitelností v rámci procesu Vulnerabilitity managementu IS

A. s cílem minimalizace (resp. snížení na akceptovatelnou úroveň) rizik bezpečnosti infomačních systémů (Důvěrnosti / Dostupnosti / Integrity)
B. s ohledem na vazbu na související proces Patch Managementu
C. s ovlivněním parametrů provádění skenování zranitelností
D. se zaměřením na zranitelnosti identifikovatelné k IP adrese a konkrétnímu zařízení (není záměrem zkoumat zranitelnosti web aplikací)
E. se zaměřením na IS s vyšší mírou komplexity a rizik
F. a její ověření praxí - Case Study

Data pro výzkum

Nezbytnou součástí výzkumu je získat důvěryhodná data v pokud možno širokém rozsahu, jak množství, tak času, tak i typů organizací, zemí světa atd.

Ještě před nástupem do studia jsem zahájil komunikaci se společností Qualys Inc. Výsledek byl kladný a podařilo se mi domluvit spolupráci s CTO Qualys Inc., panem Wolfgangem Kandekem. ***Vzhledem k tomu, že pan Kandek změnil zaměstnavatele, snažím se pokračovat v jednání s jeho nástupcem. Prozatím bezúspěšně a stanovisko je spíše negativní.***

S nástrojem QualysGuard mám dlouholeté zkušenosti, proto doufám, že se postoj společnosti změní, minimálně potřebuji jejich finální stanovisko.

První kontakt směrem ke konkurenční společnosti Tenable byl prozatím neúspěšný.

Další společnosti jsem nekontaktoval, přesto možnosti stále ještě existují.

V případě, že se nepodaří získat uvedená data, zaměřím práci na druhý její pilíř, kterým je Threat Intelligence a „Laws of Vulnerabilities" vyhodnotím z pohledu použitelnosti. Threat intelligence data bude možné využít z Open Threat Exchange zdrojů.

Přínos práce

Jelikož první přínos, kterým bylo na základě dat přehodnotit a obohatit zákonitosti zranitelností je ohrožen, bude nutné se více soustředit na druhý pilíř.

Ten se opírá o fakt, že při zkoumání existujících pramenů, týkajících se prioritizace zranitelností jsem došel k předběžnému závěru, že **dostupné vědecké práce se nezabývají problematikou komplexně a nenazírají na řízení zranitelností a jejich prioritizaci optikou řízení rizik.**

Obvykle se v rámci dostupných prací rekapitulují hodnocení úrovně zranitelností a jejich dostatečnosti či nedostatečnosti nebo aspekty, které se zabývají kontextem organizace a možných dopadů, což je velice zajímavé, ale dle mého názoru zde **chybí pohled na úrovně hrozeb,** které organizaci, resp. IS organizace, bezprostředně hrozí.

Proto velmi zajímavou výzvou bude, zda se podaří korelovat data o zranitelnostech s daty o hrozbách, a to jak celkově, tak po ekonomických sektorech a případně dle dalších atributů společností, tedy propojení na data Threat Intelligence.

Na základě analyzovaných dat je mým plánem vytvořit **metodiku prioritizace zranitelností** a definovat její doporučenou aplikovatelnost dle typu rozsahu organizace, jejíž součástí bude, pokud to bude možné a účelné, definovat indikátory účinnosti procesu řízení zranitelností (KPI) pro organizace celkově a v různých ekonomických sektorech. Tuto metodiku hodlám ověřit v praxi formou případové studie.

Harmonogram

- Průběžné shromažďování a studium dostupných zdrojů „state of the art" prioritizace zranitelností - doposud
- Jednání se společností QUALYS Inc. o poskytnutí dat - probíhá
- Získání a úvodní analýza dat o zranitelnostech - co lze vytěžit:11/2017 (Zpožděno)
- Informace - zdroje „state of the art": 10/2017 (nutno aktualizovat)
- Získání a úvodní analýza dat o hrozbách - threat intelligence: 11/2017 (Zpožděno)

V tomto bodě jsem požádal školitele a oficiálně požádám o přerušení studia, abych získal více času na změnu zdroje dat.

- Zpřesnění formulace výzkumných otázek: 01/2018
- Zpracování části disertace „state of the art": 02/2018
- Zpracování a vyhodnocení datových podkladů: 06/2018
- Testování závěrů prostřednictvím case study: 12/2018
- Publikace předběžných závěrů práce 10/2018
- Přehodnocení, revize, vývoj „state of the art" 02/2019
- Konečné zpracování disertační práce 05/2019