PREZENTACE DISERTAČNÍ PRÁCE PRO OBOROVOU RADU

Ladislav Hanzlíček

Praha 28.11. 2017

Prioritization of vulnerability remediation using laws of vulnerabilities and threat intelligence

PRO KOHO?

- Organizace, které dospěly k aktivnímu řízení zranitelností
  - … a které bojují s prioritizací jejich oprav.

CÍLE

- **Cílem práce je navrhnout metodiku prioritizace odstraňování zranitelností v rámci procesu Vulnerability Managementu IS**
  - s cílem minimalizace (resp. snížení na akceptovatelnou úroveň) rizik bezpečnosti infomačních systémů (Důvěrnosti / Dostupnosti / Integrity)
  - s ohledem na vazbu na související proces Patch Managementu
  - s ovlivněním parametrů provádění skenování zranitelností
  - se zaměřením na zranitenosti identifikovatelné k IP adrese a konkrétnímu zařízení (není záměrem zkoumat zranitelnosti web aplikací)
  - se zaměřením na IS s vyšší mírou komplexity a rizik
  - a její ověření praxí - Case Study

AMBICE METODIKY I

- I mezi zranitelnostmi s nejvyšší kritičností lze prioritizovat tak, aby bylo minimalizováno riziko pro organizaci

AMBICE METODIKY II

- Zákonitosti zranitelnosti stále platí

The Laws of Vulnerabilities

Half-life – Vulnerability half-life is 19 days on external systems and 48 days on internal systems; it doubles with lowering degrees of severity.

Prevalence – Half of the most prevalent critical vulnerabilities are replaced by new vulnerabilities each year.

Persistence – The life spans of some vulnerabilities are unlimited.

Focus – Ten percent of critical vulnerabilities cause nearly all exposure.

Exposure – The time-to-exploit cycle is shrinking faster than the remediation cycle.

Exploitation – Nearly all damage from automated attacks is during the first 15 days of outbreak.

Source: Qualys

AMBICE METODIKY III

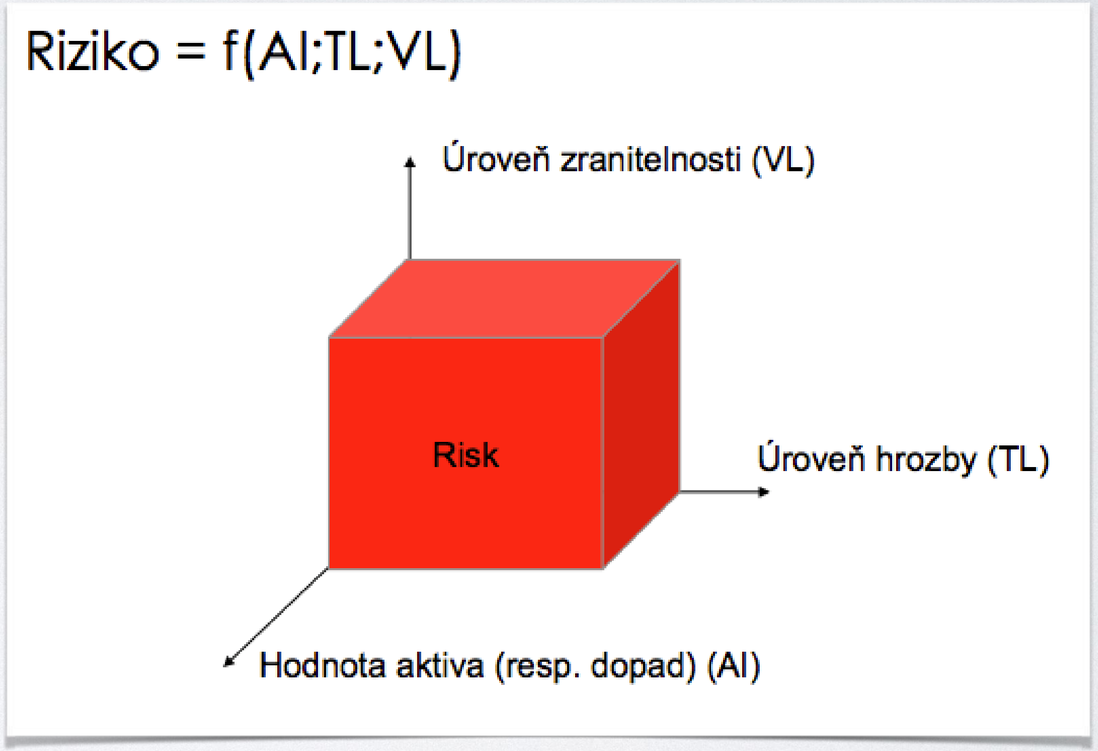
- Rozvoj Threat Intelligence může značně přispět k prioritizaci zranitelností

AMBICE METODIKY IV

- Organizace do určité velikosti / složitosti IS zvládnou prioritizovat a ostraňovat zranitlenosti s pomocí základních metod.

AMBICE METODIKY V A HLAVNÍ PŘÍNOS

- Doposud žádný zdroj „state of the art“, poznání, který jsem měl k dispozici se nedíval na prioritizaci zranitelností optikou řízení rizik tak, aby bral do úvahy komplexně:
  - úroveň zranitelnosti
  - úroveň hodnoty aktiva (resp. potenciálního dopadu)
  - úrověň hrozby



RISK ANALYSIS CONSULTANTS

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
- Informace - zdroje „state of the art“: 01/2018
- Získání a úvodní analýza dat o hrozbách - threat intelligence: 03/2018
- Zpřesnění formulace výzkumných otázek: 05/2018
- Zpracování části disertace „state of the art“: 06/2018
- Zpracování a vyhodnocení datových podkladů: 09/2018
- Testování závěrů prostřednictvím case study: 03/2019
- Publikace předběžných závěrů práce 01/2018
- Přehodnocení, revize, vývoj „state of the art“ 03/2019
- Konečné zpracování disertační práce 06/2019


how
which
why
when
what
where
who