Zkušenosti s realizací penetračních testů

Spolupráce Kraje Vysočina se sdružením Cesnet

Prosinec 2017

Petr Pavlinec, odbor informatiky KrÚ Kraje Vysočina

Kraj Vysočina

cesnet

Jak to celé vzniklo?

2001 – Vznik samostatných krajů

2003 – Žádost Kraje Vysočina o připojení k Cesnet2

2004 – zřízení linky Pardubice-Jihlava, podpis smlouvy o spolupráci a nepřímém připojování

2005 – Podpis smlouvy o zabezpečení uzlu Cesnet2

Krajská síť ROWANet distribuuje služby Cesnetu do prvních 8 mi měst na Vysočině

2006 – Přístup Kraje Vysočina k síti EDUROAM (50 AP)

2011 – Získání PI IP rozsahu, přechod na IPv6, smlouva o propagaci PI s Cesnetem

Spolupráce s CSIRT.CZ na projektu eCrime Vysočina

2013 – Instalace projektu eIGeR a CERIT-SC v nové budově KrÚ

Realizace spoje Cesnet2 - Bohdaneč (MVČR)

Kraj Vysočina

cesnet

Jak to celé vzniklo?

2014 – Smlouvy o využití linky Cesnet Jihlava-Humpolec, příprava projektu CzechLight

Aktivní využívání eIGeR pro potřeby záloh a archivace

2015 – Spolupráce při zapojení kraje do projektu FENIX

Zapojení kraje do projektu FTAS

2016 - Společná příprava podmínek pro čerpání dotací z IROP (Vnitřní konektivita škol)

2017 – Spolupráce s FLAB – penetrační testy

Krajský FTAS server, regionální řešení pro RADIUS...

A společné semináře, školení, konzultace...

Penetrační testy - zadání

- **Součást implementace opatření při zavádění ISMS a obhájení ISO27001**
- **Smlouva:**
  - kdo bude testovat (jmenovitě kvůli NDA)
  - odkud bude testováno (konkrétní IP adresy)
  - co bude testováno (konkrétní IP adresy)
  - kdy bude testováno (nejen z pohledu období, ale i z pohledu časových oken)
  - cíle testování

Penetrační testy - cíl

Cíle testování aneb odpovědět na otázky:

- Lze získat neoprávněný přístup k službám/datům/systémům?
- Lze neoprávněně modifikovat/zničit data?
- Lze narušit dostupnost služeb/systémů?
- Lze získat autentizační údaje?
- Lze zneužít infrastrukturu k útokům na sítě a služby jiných institucí?
- Existují zranitelnosti či techniky sociálního inženýrství, které mohou vést k předchozím bodům?

Penetrační testy - průběh

Průběh testů:

- Testování probíhalo cca 1,5 měsíce
- Důležité informační systémy byly důkladně otestovány
- Všechny nálezy byly profesionálně prezentovány
- 123 zranitelností všech kategorií
- Některé kroky administrátory odhaleny
- Nejzávažnější nalezené nedostatky byly identifikovány v těchto oblastech: zpracování webových aplikací, segmentace sítě a řízení přístupu a politika hesel.

Penetrační testy - výsledky

Výstupy z pohledu IT kraje

- Přes velkou snahu o omezení spustitelnosti aktivního kódu z dokumentových formátu byl útok touto cestou úspěšný (PDF)
- Obrovské množství webových aplikací a služeb znamená značné riziko pro vnitřní služby (zranitelnost aplikací, vývojářské chyby)
- Snadná napadnutelnost úředních procesů (formy phisingu)
- Překvapivě méně úspěšné sociální inženýrství na běžných uživatelých
- Existence nezdokumentovaných a zneužitelných backdoorů u dodavatelských systémů
- Politika hesel není nikdy dost přísná. Nereálné bez podpůrných systémů (vícefaktor, PAM, ...)

Penetrační testy - výsledky

Výstupy z pohledu manažerského a lidského

- Přístup FLABu byl profesionální
- Závěry a jejich detailní technická prezentace byla pro některé admini a manažery šok
- Nemalé riziko ve ztrátě motivace (hlavně u vývojářů)
- Lidský tlak na manažera bezpečnosti
- Nezbytnost práce s psychologickou složkou celých testů, prezentace výsledků a následných opatření
- Extrémně důležitá role top-managementu – vysvětlení, závěry, výstupy

Penetrační testy - opatření

Jaká opatření realizujeme

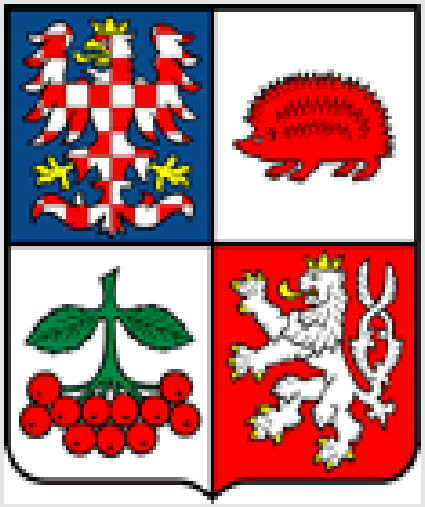
- Záplatujeme
- Zásadně měníme politiku hesel (nasazení PAM)
- Zmenšujeme náš „povrch“ na internetu
- Větší kontrola vývoje a správa zdrojového kódu
- Připravujeme mikrosegmentaci sítě
- Připravujeme zásadní reinženýring AD/LDAP
- Dokumentuje, testujeme ...
- .... ä chystáme se na další penetrační testy ;-)

ISO 27001

Kraj Vysočina

cesnet

Kontakt



Krajský úřad kraje Vysočina

Žižkova 57, Jihlava 587 33

www.kr-vysocina.cz

www.kr-vysocina.cz/it

www.rowanet.cz

Ing. Petr Pavlinec – vedoucí odboru informatiky

- pavlinec.p@kr-vysocina.cz