Nasazení nových modulů McAfee

Seminář CIV (nejen) pro lokální správce

Ing. Petr Žák

Obsah

I. Úvod aneb ePolicy Orchestrator
II. Nové moduly: McAfee Endpoint Security
III. Politiky pro nové moduly
IV. Přechod na nové moduly
V. Diskuse a praktické ukázky
   - Ptejte se kdykoli v průběhu prezentace
   - Pamatujte/pište si dotazy typu “jak se dělá x?”

Epizoda I.

Úvod do McAfee na ZČU

Centrální správa

- ePolicy Orchestrator (ePO)
  - Centrální server
  - apollon.zcu.cz, epo.zcu.cz
- System Tree
  - Stromová struktura systémů, každý vidí “svoji” část
- Bezpečnostní politiky a client tasks
  - Chování a úkoly
- Repozitář softwaru
- Logy, dashboardy, dotazy, reporty...

Koncové stanice

- McAfee Agent
  - Lokální SW, zprostředkovává komunikaci s ePO
  - Zajišťuje provedení serverem definovaných úkolů
- Použití
  - Správce: vytvoření instalačního balíčku na ePO, instalace na daný stroj
  - Agent: zahájení komunikace, získání úkolů a politik, instalace a konfigurace dalšího softwaru
- Zařazení systému do System Tree
  - Vygenerování balíčku Agenta pro příslušnou skupinu
  - Nastavení pravidel na serveru (dle IP, hostname…)

Možnosti lokálního správce

- Přístup do ePO na žádost
- Sledování a správa “vlastních” systémů
  - Vlastní část System Tree
  - Nasazování a ovládání agentů
  - Definice a přiřazení politik a client tasks
  - Využívání logů, dashboardů, dotazů, reportů…
    - Vytvoření CIVem na žádost
- Centrální správa CIV
  - Repozitář
  - Správa uživatelských účtů
  - Správa serveru...

Epizoda II.

Seznámení s MES

Dobrý den, já jsem MES

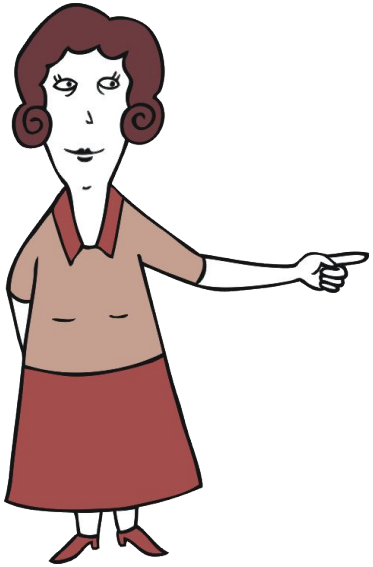
- MES = McAfee Endpoint Security
  - Endpoint Security Threat Prevention
  - Endpoint Security Firewall
  - Endpoint Web Control
- Náhrada za
  - VirusScan Enteprise (VSE)
  - Host Intrusion Prevention System (HIPS)
  - Site Advisor (na ZČU jsme nepoužívali)

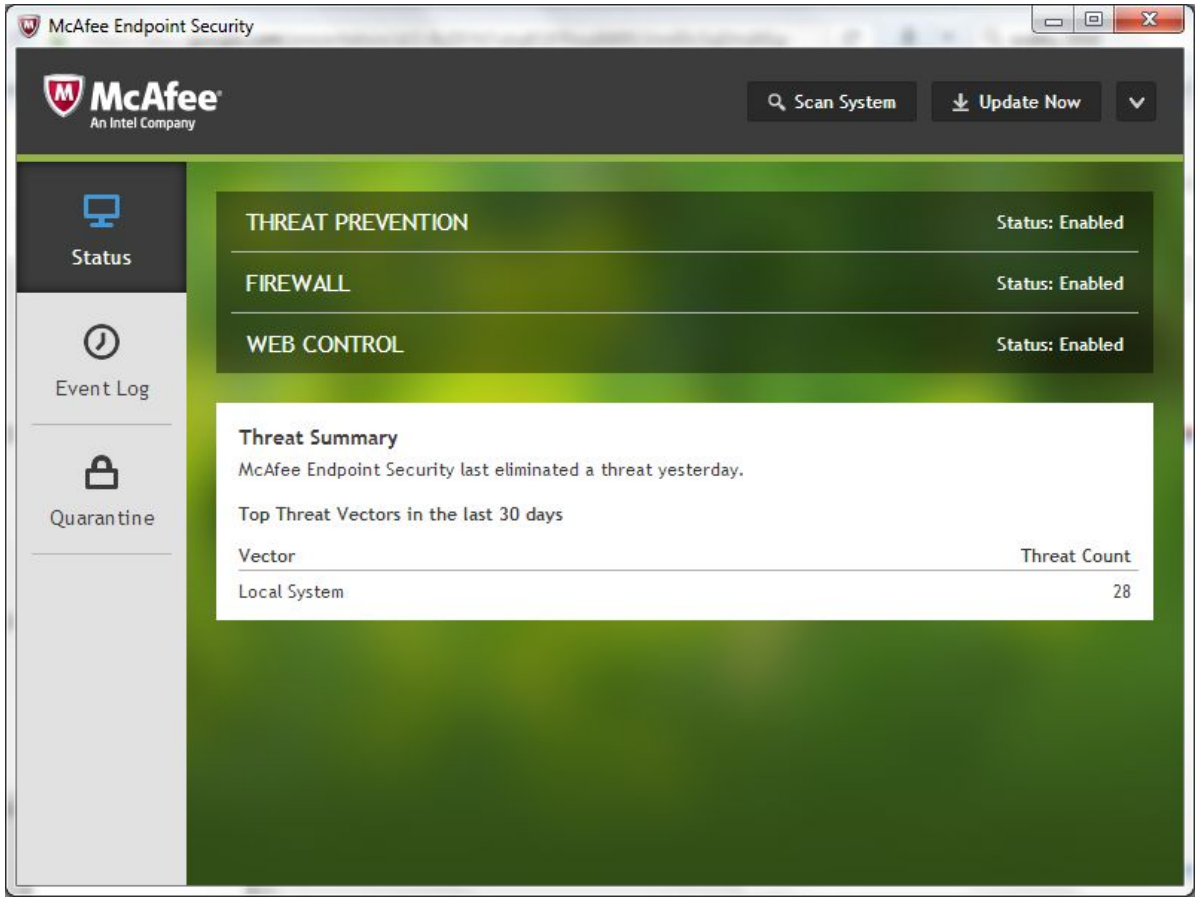
Proč ❤ MES

- Udržitelnost provozu
  - Oficiální náhrada za starší moduly
  - Podpora Windows 10
- Konfigurace v ePO
  - Přehlednější
  - Propracovanější
- Bezpečnostně
  - Širší možnosti konfigurace
  - Lepší funkčnost
  - Global Threat Intelligence
    - Reputační databáze souborů, webů, zařízení...

Proč ❤ MES

- Vylepšené GUI (plná lokální konfigurace!),



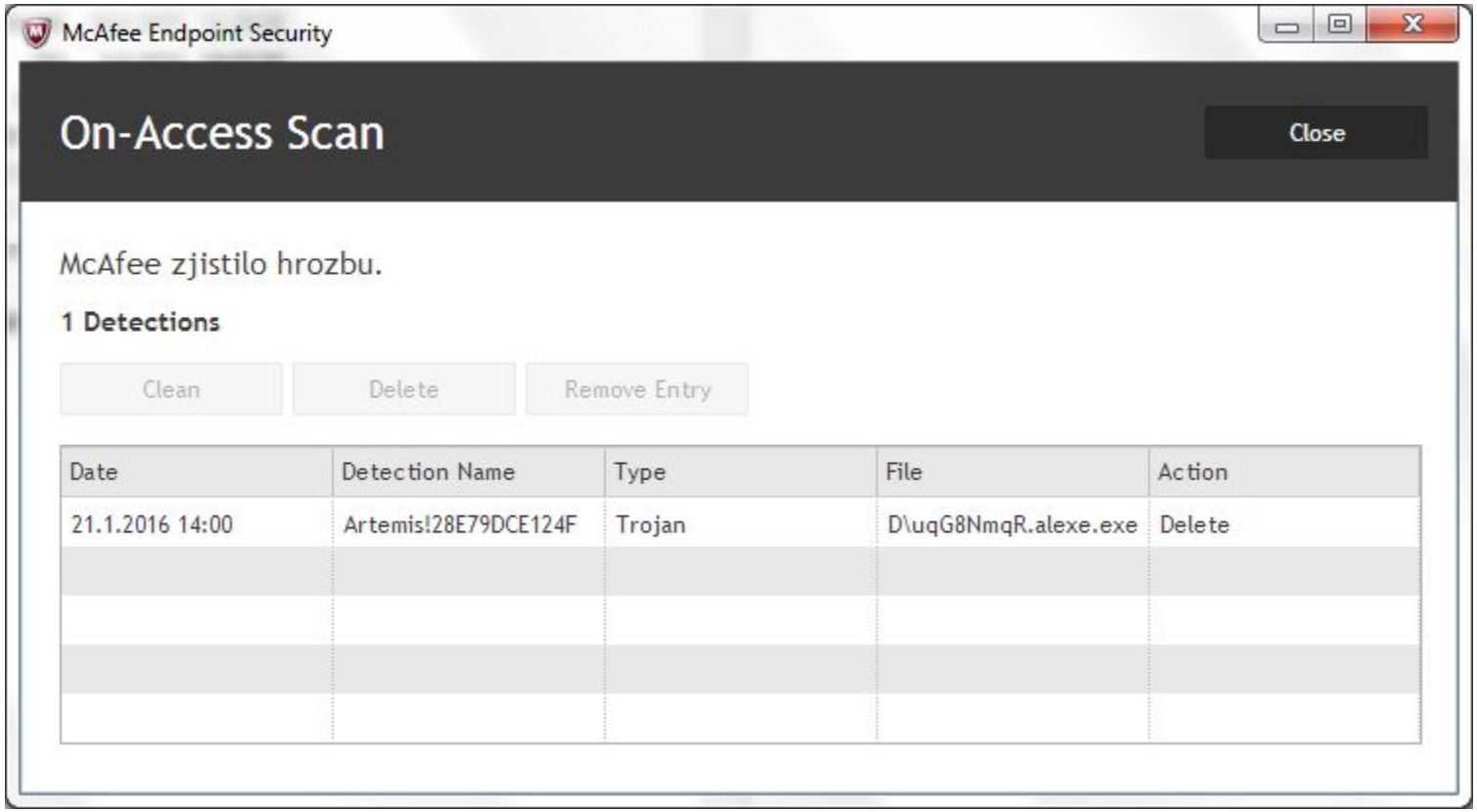


Komponenta Threat Prevention

- On-Access Scan
  - Antivirový štít
  - Čtení/zápis souborů
  - ScriptScan
- Access protection
  - Omezení přístupů (registry, soubory, ...)
- Exploit Prevention
  - DEP (Data Execution Prevention)

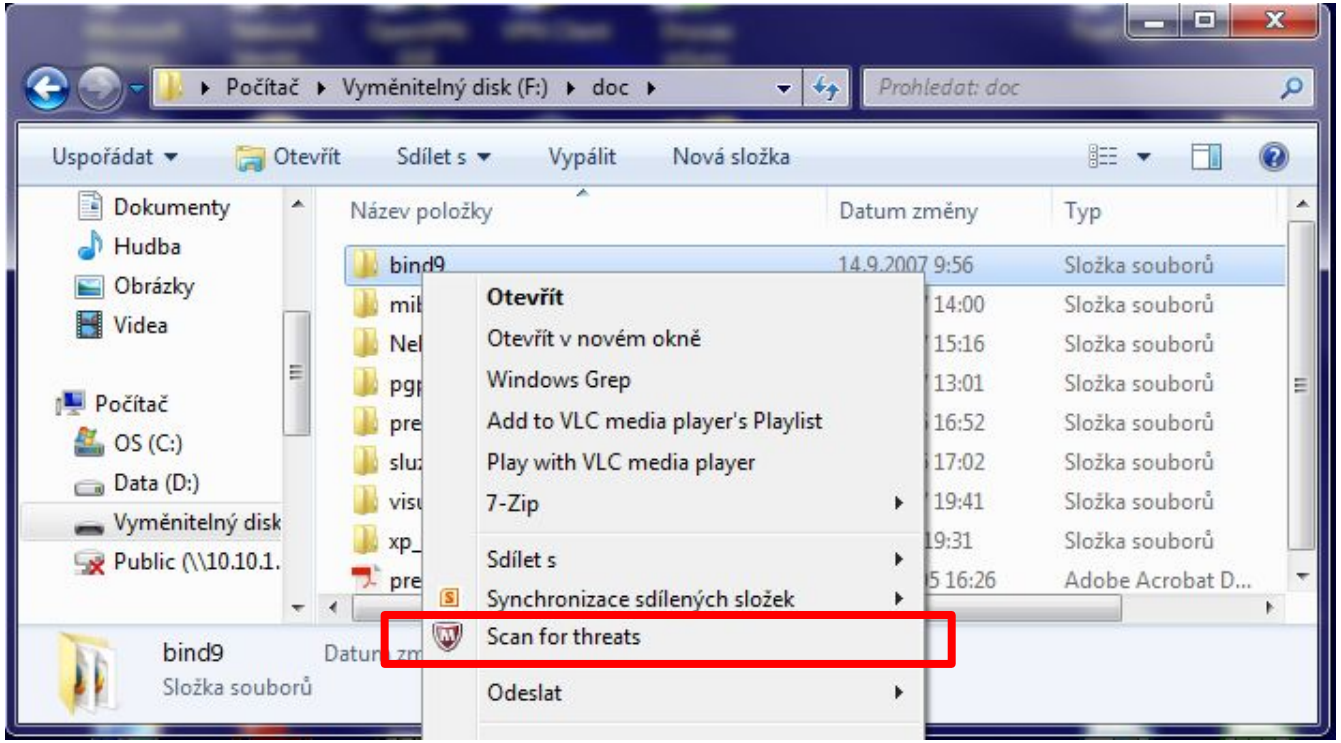
Komponenta Threat Prevention

- On-Access Scan (upozornění na zásah)

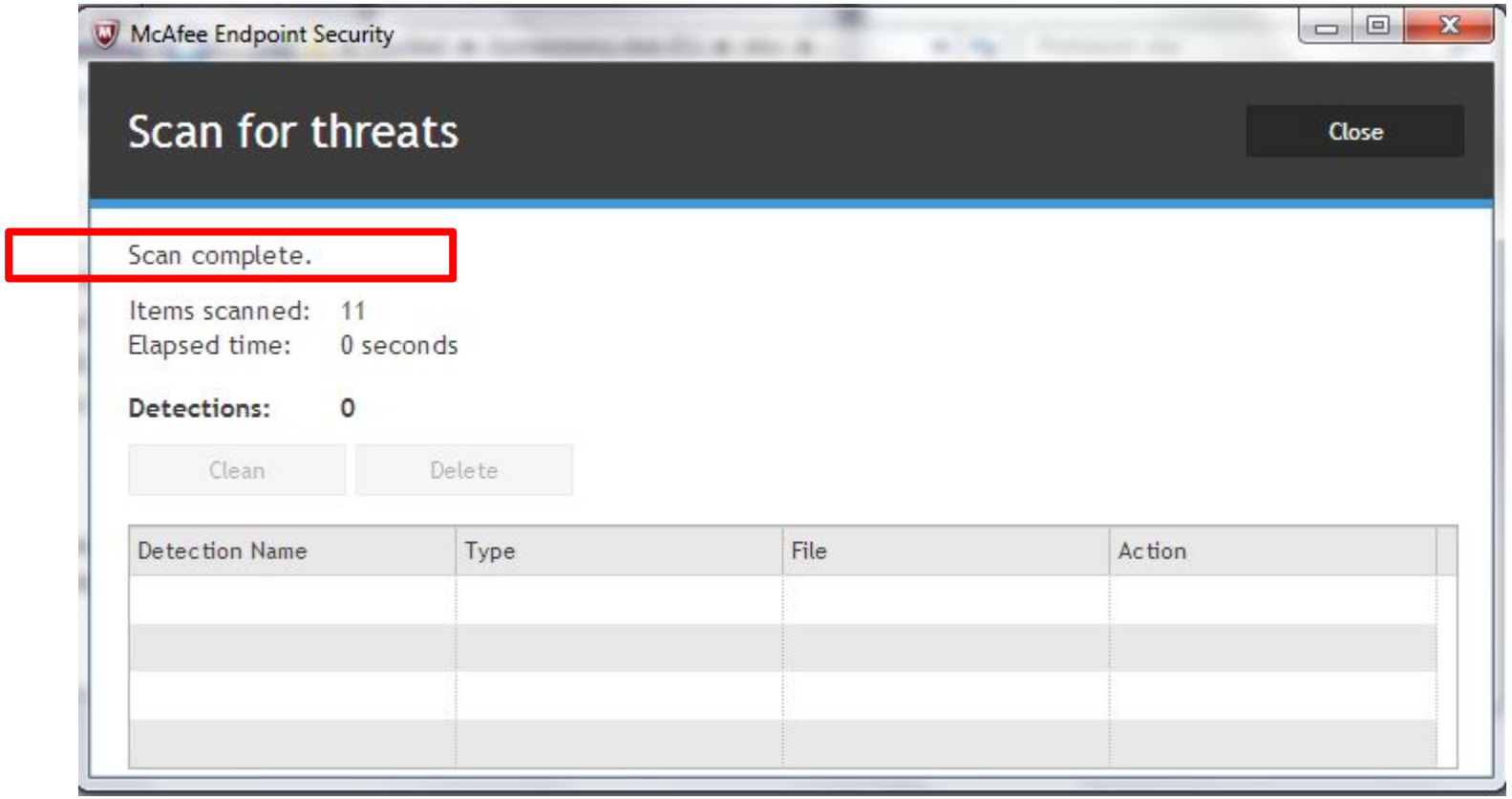


Komponenta Threat Prevention

- On-Demand Scan (vyžádání uživatele)
  - Pravé myší tlačítko - kontextové menu



Komponenta Threat Prevention



Komponenta Firewall

- Klasický aplikační stavový firewall
  - IP adresa
  - Protokol
  - Port
  - Aplikace
  - Možnost časového omezení
- Doménový firewall (DNS)
  - Pro odchozí spojení
  - Specifikace domény
  - Blokovaná komunikace (např. phishing)

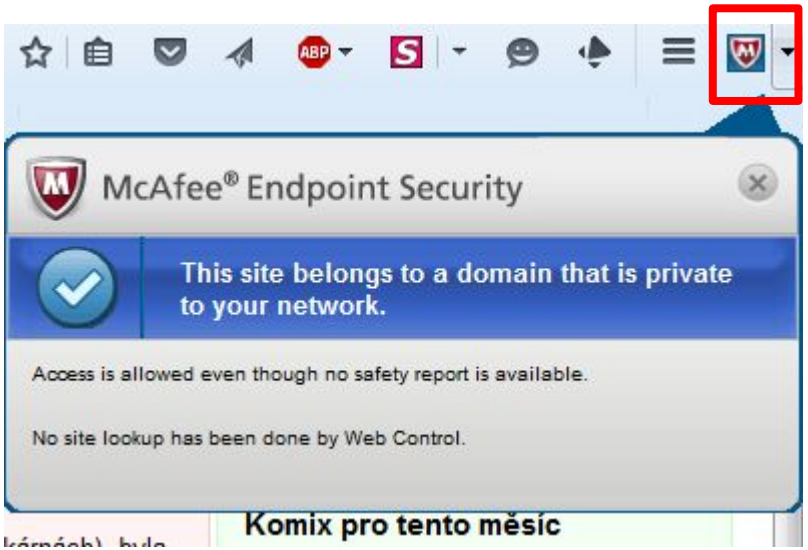
Komponenta Web Control

- Omezení přístupu na webové stránky
  - Špatná reputace
  - Vlastní blacklist
- Možnost definice whitelistu
  - Např. *.zcu.cz
- Podpora prohlížečů
  - Internet Explorer, Mozilla Firefox, Google Chrome
  - Neumí (zatím) Edge
  - Lze zakazovat prohlížeče

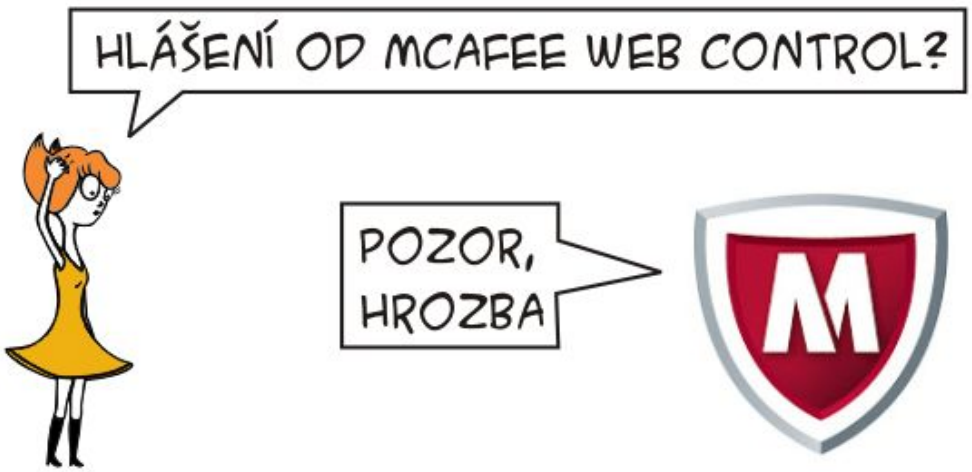
Komponenta Web Control

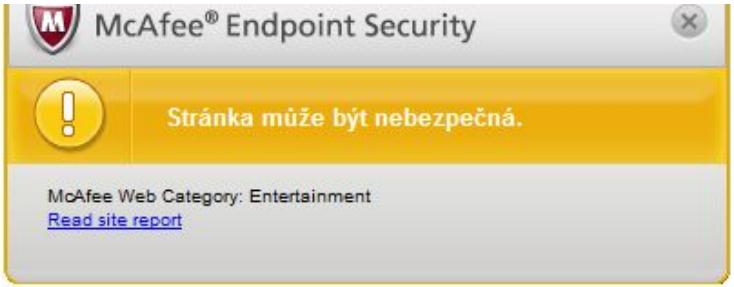
- Hodnocení stránek
  - Šedá = nevím, neznám
  - Modrá = na správcem definovaném whitelistu
  - Zelená = zkontrolováno, bezpečné
  - Žlutá = zkontrolováno, podezřelé
  - Červená = zkontrolováno, nebezpečné
- Reakce
  - V pořádku
  - Upozornění, možnost projít
  - Blokování, bez možnosti projít

Komponenta Web Control



Komponenta Web Control





Stránka může být nebezpečná.

cs.nametests.com

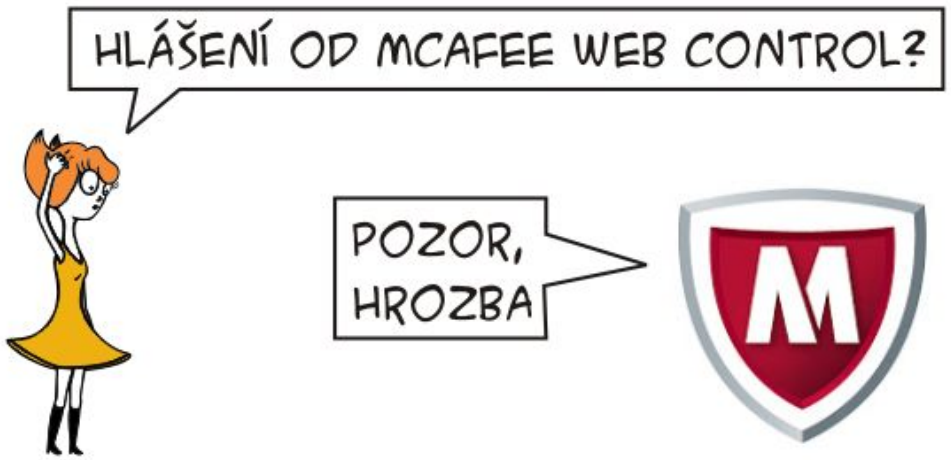
A security risk is posed by this site.

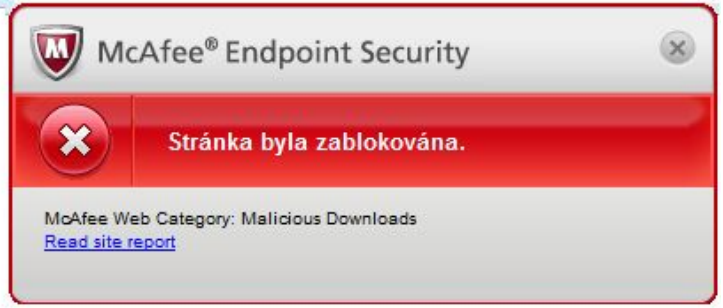
McAfee Web Category: Entertainment
McAfee Security Rating: Yellow

Cancel Continue

Powered By: McAfee Endpoint Security

Komponenta Web Control





Stránka byla zablokována.

exploitpack.com

An unacceptable security risk is posed by this site.

McAfee Web Category: Malicious Downloads
McAfee Security Rating: Red

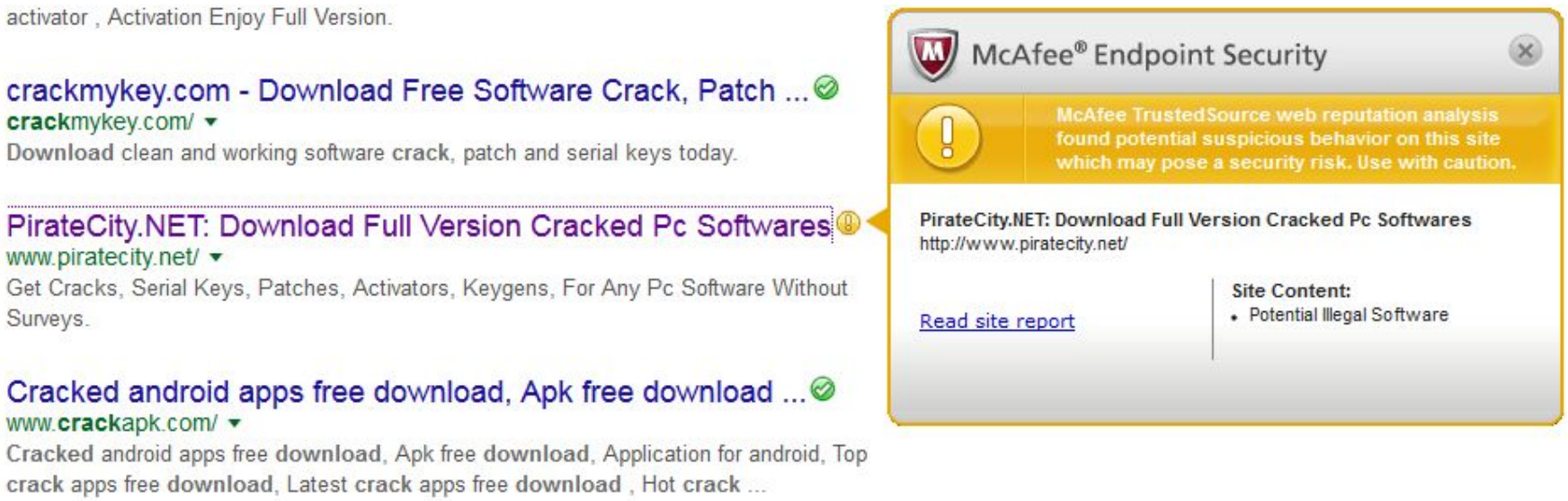
OK

Powered By: McAfee Endpoint Security

McAfee

Komponenta Web Control

- Asistence u vyhledávání



Platformy

- Windows
  - Otestováno na všech podporovaných verzích
    - Opravdu nejvyšší čas se zbavit XP
- Ostatní platformy
  - Vysoce...experimentální
  - Virus Scan Enterprise for Linux
    - Jen 64b, ne všechny verze všech distribucí
    - Potřeba několik ošklivých hacků
    - On-Access Scan + lokální konfigurace
  - MES for Mac
    - Zatím bez úspěchu

Epizoda III.

Politiky pro MES

Rychlý úvod do politik

- Politika = definice chování daného modulu
  - Vypnutí a zapnutí různých funkcí
  - Pravidla firewallu
  - Parametry antivirového testu
  - Blacklisty a whitelisty webů
  - …
- Veškeré produkty McAfee konfigurovány kompletně pomocí přiřazení politik vytvořených na ePO serveru

Defaultní politiky

- Existují pro každý typ politiky
- Vytvořené a **aktivně spravované** ClVem
  - Testování, ladění, podpora
  - Reakce na aktuální situace a hrozby (phishing…)
- Ve většině případů postačující a vyhovující

Typy defaultních politik

- Global-standard
  - Defaultní pro lokálně spravované stroje
  - Konfigurace dle CIVu (“nejlepší vědomí a svědomí”)
  - Možnost lokálně měnit nastavení přes GUI
- Global-Orion
  - Defaultní pro stanice ve správě CIVu (IS)
  - Stejná konfigurace jako standard
  - Bez možnosti lokálních změn přes GUI
- Global-off
  - Daný modul či funkčnost kompletně deaktivována
  - Pouze typy politik, kde to má smysl

Vlastní politiky

- Nevytvářejte, pokud to není opravdu nutné
  - Defaultní politika => méně práce pro všechny
  - Přehlednost, jednoduchost, ladění chyb
- Pokud vytváříte, dodržuje konvence
  - Jméno začíná zkratkou fakulty či oddělení
  - Např. CIV - ucebny - UI666
- Kdy mají smysl?
  - Pravidla firewallu
  - Blokované a povolené weby
  - Speciální software či skripty
  - ...ale jste v tom sami (příp. konzultujte s CIVem)

Přenos současných politik

- “Mám něco nastavené ve VSE/HIPS, budu to muset klikat znovu?”
  - S trochou štěstí ne :-)

- Pravidla firewallu
  - Převedení politiky s FW pravidly pro HIPS na politiku pro MES připraveno
  - Provede CIV AUP na vyžádání
- Ostatní politiky
  - Individuálně po dohodě

Epizoda IV.

Přechod a nasazení

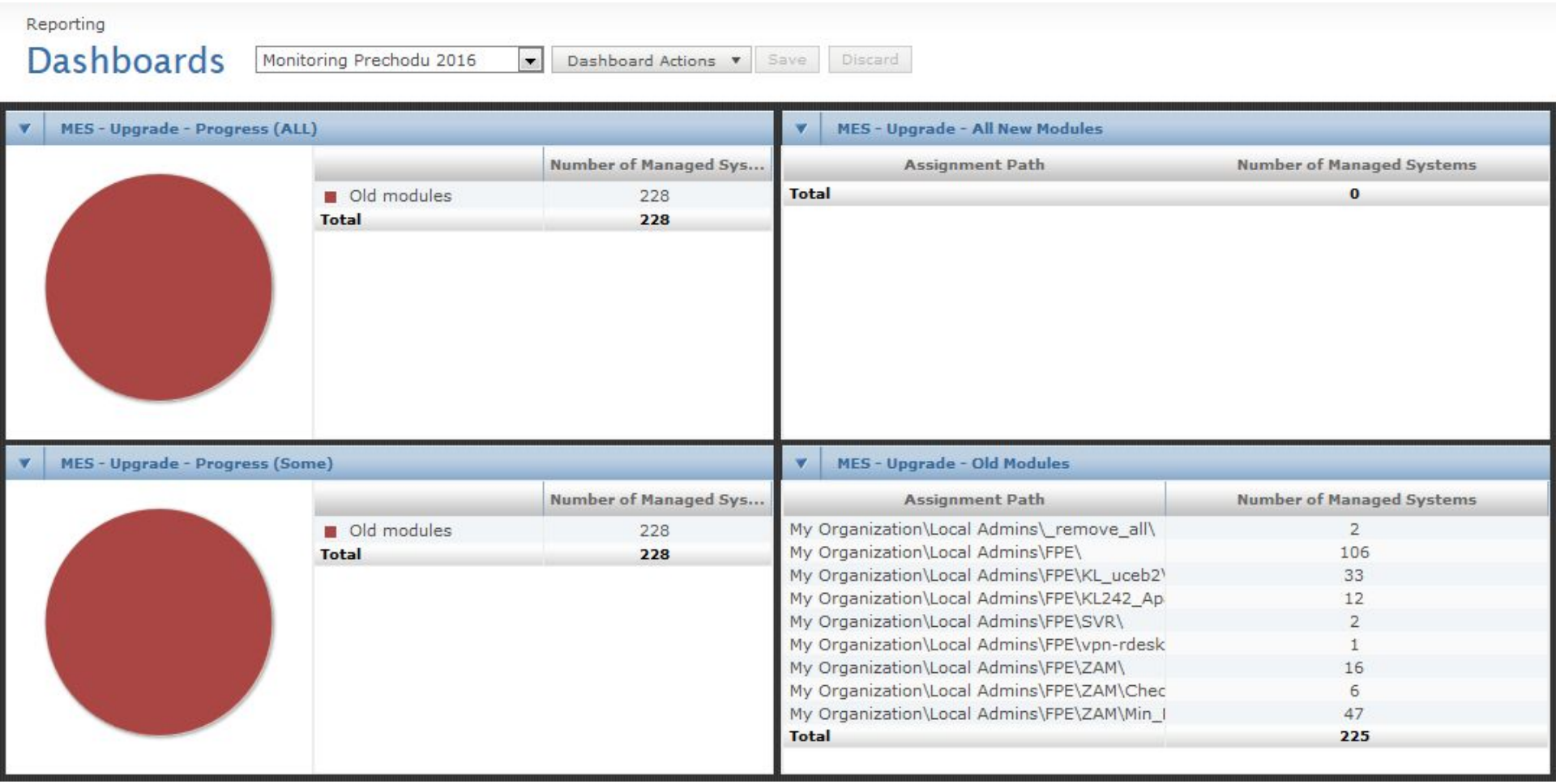
Instalační client tasks

- Client task = úkol, zadaný serverem klientovi
  - Např. spuštění testu, aktualizace nebo **instalace nového sw Agentem**
- Přechod na MES
  - Deaktivovat či odebrat instalační tasky VSE a HIPS
  - Přiřadit Agent Product Deployment client task:
    - Install - MES (Full) - všechny moduly
    - Install - MES (TP FW) - bez Web Control
  - Jako na frontě...počkáme a uvidíme.
- Změny provede AUP na Vaši žádost

Monitoring přechodu na MES

- Dashboard na ePO
  - Monitoring Prechodu 2016
  - Každý vidí “svoje” systémy
    - Opravdu? :-)
- Jiné dashboardy, dotazy či reporty
  - Individuálně na žádost
  - Platí nejen v tomto případě

Dashboard před přechodem na MES



Dashboard během přechodu na MES

Reporting

Dashboards

Monitoring Prechodu 2016 | Dashboard Actions | Save | Discard

MES - Upgrade - Progress (ALL)

	Number of Managed Sys...
ALL new modules	714
Old modules	138
Total	**852**

MES - Upgrade - All New Modules

Assignment Path	Number of Managed Systems
My Organization\CIV\Computer Labs\	125
My Organization\CIV\Computer Labs\CD203	27
My Organization\CIV\Computer Labs\EP207	15
My Organization\CIV\Computer Labs\HJ3xx'	58
My Organization\CIV\Computer Labs\Kiosks	6
My Organization\CIV\Computer Labs\UI201'	21
My Organization\CIV\Computer Labs\UI202'	20
My Organization\CIV\Computer Labs\UI203'	12
My Organization\CIV\Computer Labs\UI505l	9
My Organization\CIV\Computer Labs\UU406	36
My Organization\CIV\Computer Labs\Virtual	5

MES - Upgrade - Progress (Some)

	Number of Managed Sys...
Some new modules	719
Old modules	133
Total	**852**

MES - Upgrade - Old Modules

Assignment Path	Number of Managed Systems
My Organization\CIV\Computer Labs\	1
My Organization\CIV\Computer Labs\CD203	3
My Organization\CIV\Computer Labs\EP1XX	1
My Organization\CIV\Computer Labs\HJ3xx'	1
My Organization\CIV\Computer Labs\UU406	1
My Organization\CIV\IS K1\	19
My Organization\CIV\IS K1\leasing\	2
My Organization\CIV\IS K1\VirusScan Only\	3
My Organization\CIV\IS K2\	3
My Organization\CIV\IS K2\leasing\	1
My Organization\CIV\IS K2\Vyjimky\	1

Harmonogram přechodu na MES

- Červen 2016 (současnost)
  - Nasazeno a otestováno na IS stanicích
  - Zahájení upgradu na lokálně spravovaných stanicích
- Červen - srpen 2016
  - Upgrade na lokálně spravovaných stanicích
  - V režii jejich lokálních správců za podpory CIV
- Září 2016
  - Povinný/CIVem vynucený upgrade zbylých strojů
- Říjen 2016
  - Ukončení podpory VSE a HIPS (i strojů s nimi!)

Řešení potíží při přechodu na MES

- Vypnout a zapnout :-)
- Vše kromě Agenta odinstalovat a znovu nainstalovat pomocí client tasks
- Zkontrolovat správné přiřazení a nastavení client tasks
- Zkontrolovat aktuálnost verze Agenta (15.6.2016: 5.0.2.333), upgradovat či reinstalovat agenta
- Požádat o pomoc CIV (via Helpdesk)

Epizoda V.

Diskuse, dotazy, workshop...