SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Praktické zkušenosti s provozováním SIEM RSA enVision

Bc. Jiří Kout, Michal Miklánek

Česká pošta s.p.

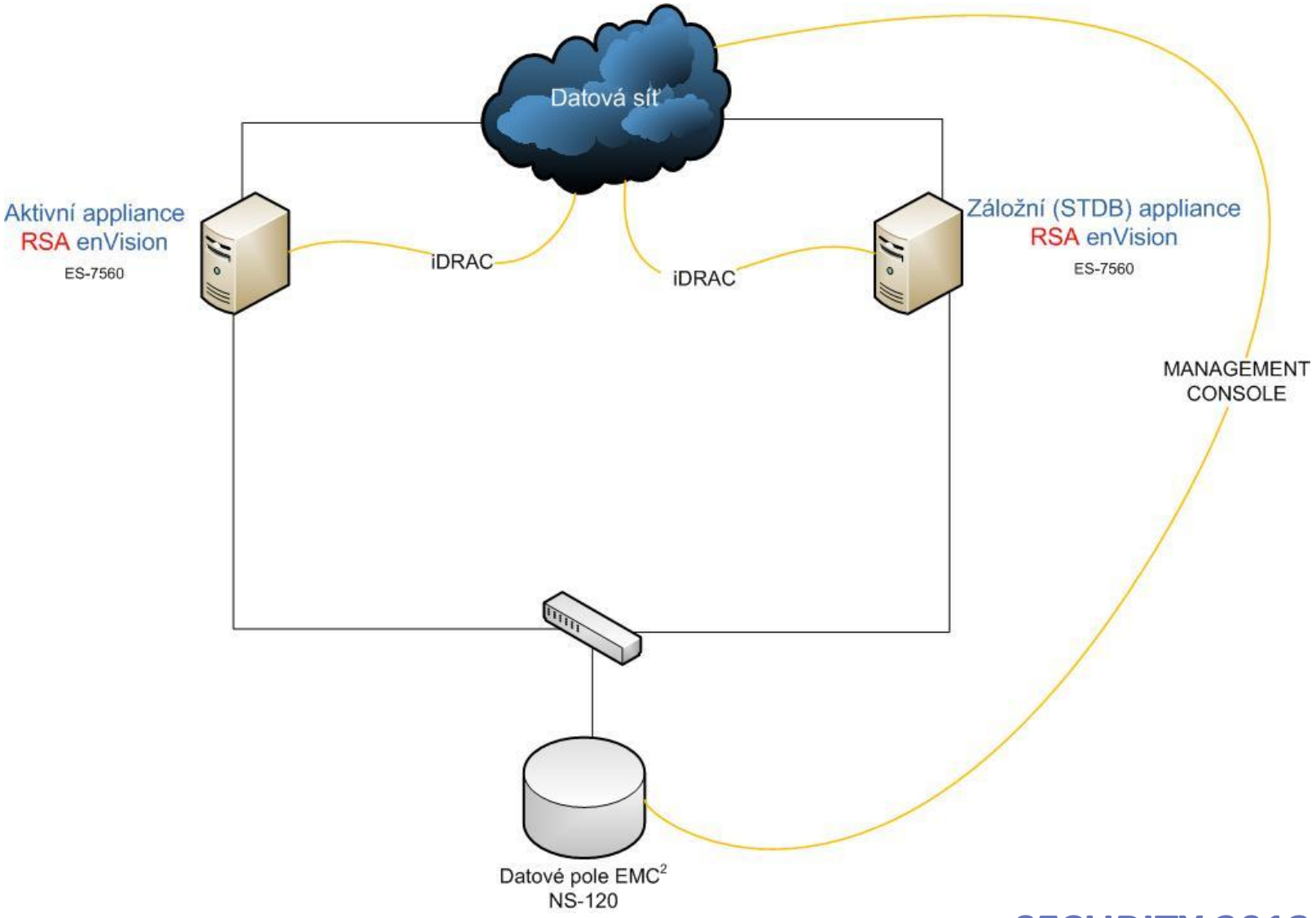
Obsah

- Historie
- Popis současného stavu
- Průběh nasazení
- Časté otázky / odpovědi

Historie nasazení SIEM v ČP

- Historie
  - SIEM pro BICT pořízen v roce 2009
  - O rok později přikoupena 2. appliance (STDB) + 7T diskové pole od EMC
  - Příprava na pseudo HA
    - V případě nefunkční appliance je připraven na instalaci druhý box (cca 5h DRP)
  - Logy jsou ukládány na EMC diskové pole
    - Kapacita pole umožňuje při současném provozu archivovat logy min. 3 roky

Historie nasazení SIEM v ČP



Současný stav

- Popis současného stavu
  - ES 7650
  - 1 Licence na 1250 zařízení / 7500 EPS
  - 7T diskové pole (po dvou letech zaplněno 8%)
  - Loguje cca 700 zařízení
    - FW
    - Páteřní switche a routery
    - Serverové operační systémy
    - Business aplikace
    - IPS
    - PROXY do internetu
    - Network Access Control
    - atd.

Průběh nasazení

- Průběh nasazení
  - Při zakoupení byla technická podpora nedostatečná
  - 1 rok proběhl s podporou technicky zdatnější, ovšem bez hlubšího zapojení security invence
  - 1 rok zcela bez podpory – pouze s Help deskem RSA, nedoporučeno
  - 1,5 roku spolupráce s podporou, která splňuje požadovanou úroveň

Otázky / Odpovědi

- *Jak dlouho trvala vlastní instalace, testování a uvedení do rutinního provozu SIEM?*
  (instalace HW, instalace SW, napojení zdrojů, konfigurace korelačních pravidel, konfigurace eskalačních workflow, reporting, testování funkčnosti)
  - Instalace HW a SW - *v řádu několika málo dnů*
  - Napojení zdrojů – *dny až týdny*
    - Může být velmi rychlé např. u syslogu nebo Windows
    - Existují i pracnější zařízení (např. FW – konfiguruje se na obou stranách)
    - Náročnější je také připojovat vlastní aplikace
  - Konfigurace korelačních pravidel, konfigurace eskalačních workflow, reporting, testování funkčnosti – *dlouhodobý proces*

Otázky / Odpovědi

- *V čem vám pomohl výrobce, v čem vám pomohl dodavatel, co zůstalo na vás?*
  - Výrobce
    - Přímý kontakt na HelpDesk výrobce není obecně doporučen. (support RSA existuje, zpravidla ovšem končí na Webexu..)
    - Návody na připojení standardních zařízení na webu RSA
  - Podpora dodavatele
    - Při zaškolení do produktu
    - Při náročnějších akcích (migrace appliance nebo diskového pole, parsování logů z vlastních zařízení, složitější korelační pravidla)
  - Vlastní úsilí
    - Korelační pravidla, připojování zařízení, pravidla pro Alerty, tvorba reportů

Otázky / Odpovědi

- *Podle jakých rolí máte nastaveno workflow? Jaké **procesní role** / **organizační útvary** pracují se SIEM? Komu je řešení SIEM primárně určeno?*
  - Administrátor enVision – 1 osoba
    - Správa uživatelů a rolí
    - Instalace opravných patchů (VAM & Source Update)
    - Vytváření pravidel pro Alerty
    - Vytváření korelačních pravidel
    - Správa a údržba plánovaných a ad-hoc reportů
  - Bezpečnostní administrátor – 3 osoby
    - Bezpečnostní dohled
    - Vyhodnocování a řešení vzniklých alertů
    - Rutinní pohled na reporty
    - Tvorba týdenních či ad-hoc výstupů pro Manažera bezpečnosti IT
  - Manažer bezpečnosti IT
    - Předkládá výstupy na týdenních poradách vedení
    - Manažerský pohled do enVision (tzv. „semafory“) se neosvědčil

Otázky / Odpovědi

- *Na co si dát pozor při implementaci a při následném provozu, čeho se vyvarovat?*
  - Implementace SIEM vyžaduje podporu širšího vedení firmy
  - Je nezbytná dobrá spolupráce mezi jednotlivými složkami IT
  - Určit priority při napojování zařízení
  - Určit správně úroveň logování
  - Připojovat zařízení postupně – dát čas na odladění
  - Vybrat vhodnou podporu dodavatele

Otázky / Odpovědi

- *Jak jste se stávajícím řešením spokojeni? Vybrali byste si znovu stávající systém? Proč?*
  - Ano
  - Dobrý poměr „cena/výkon“
  - Drobné výhrady k reportingu, k řešení HA, ke grafickému provedení webového GUI. Není zpracováváno netflow. Řešeno v následující generaci SIEM od RSA.

Otázky / Odpovědi

- *Z jakých zdrojů / systémů sbíráte log záznamy? Máte nějaké doporučení, jakými typy zdrojů / systémů začít?*
  - Syslog
  - Windows Service
  - SDEE
  - LEA Service
  - ODBC Service
  - File Reader
- *Používáte i vlastní specifické korelace?*
  - Osvědčilo se i v případě jednoduchých alertů používat vlastní korelační pravidla. Výhoda snadného exportování/importování. Korelace od výrobce používáme spíše pro inspiraci

Otázky / Odpovědi

- *Plánovaný rozvoj?*
  - Aktualizace UNIX politik
  - Politiky aplikačních serverů

Otázky / Odpovědi

- *Používáte jiné nástroje mimo webového GUI*
  - Event Explorer (Incident Management)
    - Umožňuje zpracovávat tzv. „Tasks“. Vzniklý alert obsahující korelační pravidlo může být převedeno na „Task“ (Incident), který zpracuje Bezpečnostní administrátor, kterému je přiřazen.
  - RSA enVision EventSource Integrator
    - „Click & go“ nástroj pro parsování neznámého logu

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Bc. Jiří Kout, Michal Miklánek

Česká pošta s.p.

Kout.Jiri@cpost.cz

Miklanek.Michal@cpost.cz