SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Hardening ICT platforem: teorie nebo praxe

Pavel Hejduk

ČEZ ICT Services, a. s.

Agenda

- ICT prostředí ČEZ ICT Services a. s.
- Hardening ICT platforem - definice
- Obvyklý přístup …
  - … a jeho omezení
  - … zhodnocení
- Lze to udělat lépe?
  - Definice politiky
  - Prosazení požadavků
  - Ověření požadavků
- Shrnutí

ČEZ ICT Services, a. s.

- Poskytovatel IT a TELCO služeb pro Skupinu ČEZ
- Provoz a rozvoj systémů ERP, CIS, TIS/GIS, …
  - 12tis. interních uživatelů
  - 15tis. koncových zařízení
  - Více jak 1000 instancí serverových OS, stovky aplikačních serverů a databází
- Poskytování ICT služeb pro
  - Integrované společnosti Skupiny ČEZ v ČR (22 lokalit)
  - Akvizice (Bulharsko, Rumunsko, Polsko, …)
  - Další majetkové účasti

Hardening ICT platforem - definice

- **Hardening** – kalení, přitvrzení, zpevnění, tvrdnutí, zatvrdnutí, tvrzení
- **Hardening ICT systémů** – proces zabezpečení ICT systémů s cílem eliminovat jejich platformní/implementační zranitelnosti
- **Hardening ICT systémů** – základní činnosti:
  - Definice politiky
  - Definice & nastavení konkrétních požadavků
  - Detekce a prioritizace zranitelností / neshod
  - Průběžné ověřování & nastavení & revize politiky

Obvyklý přístup … (příklad)

- Definice politiky
  - „Máme ji, je na webu …“
- Definice & nastavení konkrétních požadavků
  - Vytvoření požadavků „na míru“
  - Posouzení dle nasazení/použití/kritičnosti systému
  - Provedení nastavení ručně přímo v systému
- Detekce a prioritizace zranitelností
  - Ručně – ověření „namátkou“
  - Skriptem / vulnerability scanner – automatizace
- Průběžné ověřování & nastavení & revize politiky
  - „Pouštím test v cronnu …“
  - Revize bezpečnostní politiky ???

(příklad) … a jeho omezení

- Definice politiky
  - Formalizace požadavků – TOP vs. systémová BP
- Definice & nastavení konkrétních požadavků
  - Posuzujeme každý implementovaný systém samostatně
  - Nastavení nelze jednoduše zobecnit - automatizovat
- Detekce a prioritizace zranitelností
  - Opakovatelnost ověření
  - Interpretace výstupů – co je důležité, vazba na SBP
- Průběžné ověřování & nastavení & revize politiky
  - Opakovatelnost & možnost srovnání výstupů
  - Životní cyklus systémové bezpečnostní politiky

(příklad) … a jeho zhodnocení

- Realizace hardeningu je kapacitně náročné
  - Dílčí nastavení pro jednotlivé systémy
  - „košaté“ výstupy z vulnerability scanneru – není zřejmé, která zjištění jsou relevantní / validní vůči SBP
- Ověřování & vyhodnocování „jednou za čas“
- Kvalita hardeningu
  - Je úměrná času, který tím trávíme
  - Definovaná politika vs. skutečný stav

Zabezpečení systémů je na rozdílné úrovni => hardening nepřináší zlepšení

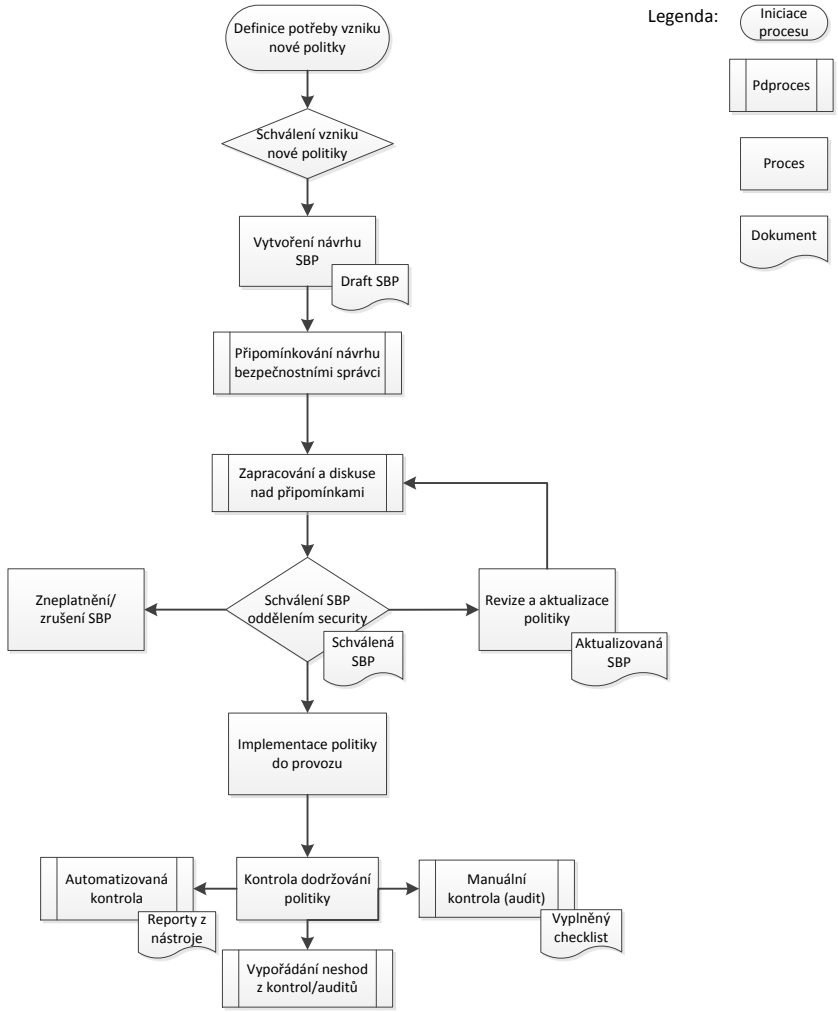
Lze to udělat lépe?

- Definice strukturované a detailní politiky (SBP)
  - Bezpečnostní požadavky – nadřazená BP
  - Platformní možnosti (omezení, zranitelnosti)
  - Celkový bezpečnostní koncept (kombinace opatření)
  - Řízení životního cyklu politiky
- Prosazení v infrastruktuře
  - Kampaň – pokrytí priorit
  - V rámci změn v IS – dopady do change managementu
- Ověření parametrů, kontrola
  - Formální ověření - checklist
  - Automatické ověření

Definice politiky

- Struktura
  - Úvod
    - Cíl politiky
    - Rozsah platnosti
    - Základní popis
    - Předpoklady
    - Metodiky a informační zdroje
    - Definice odpovědnosti
  - Procesy bezpečné správy
    - Aktualizace systémů – patch management
    - Monitoring provozu
    - Systémová dokumentace
    - Změny v konfiguraci
  - Bezpečnostní požadavky (genericky)
    - Popis (stručný popis)
    - Riziko (definuje prioritu opatření)
    - Nastavení (postup pro nastavení a kontrolu)
  - Security checklist – samostatná příloha politiky

- Životní cyklus



Příklad bezpečnostního požadavku

ID202 Politiky pro Event Log

Popis

Optimalizace nastavení politik pro záznamy (Event log). Optimalizace velikosti a přístupů k záznamům.

Riziko

Nedostatečná velikost logů může zapříčinit, že záznamy budou v případě útoku přepsány a nebude možno identifikovat aktivity a průběh útoku.

Nastavení

Zkontrolovat, případně nastavit (pokud tomu tak není), následující logování událostí pomocí GPO u member serverů:

```
AD Users and Computers -> [OU_with_servers] -> Properties -> Group Policy -> [GP_for_servers]
-> Edit -> Computer Configuration -> Windows Settings -> Security Settings -> Event Log

Nastavení:

Maximum Security Log size: 131072
Maximum Security Log size: 131072
Maximum Security Log size: 131072

Prevent local guests group from accessing application log: Enabled
Prevent local guests group from accessing Security log: Enabled
Prevent local guests group from accessing system log: Enabled

Retention method for security log: Overwrite events as needed
Retention method for system log: Overwrite events as needed
Retention method for application log: Overwrite events as needed
```

Zkontrolovat, případně nastavit, následující nastavení u standalone serverů:

```
Eventvwr.msc
Seccurity, systém, application -> Properties

Maximum Security Log size: 131072
Maximum Security Log size: 131072
Maximum Security Log size: 131072

Retention method for security log: Overwrite events as needed
Retention method for system log: Overwrite events as needed
Retention method for application log: Overwrite events as needed
```

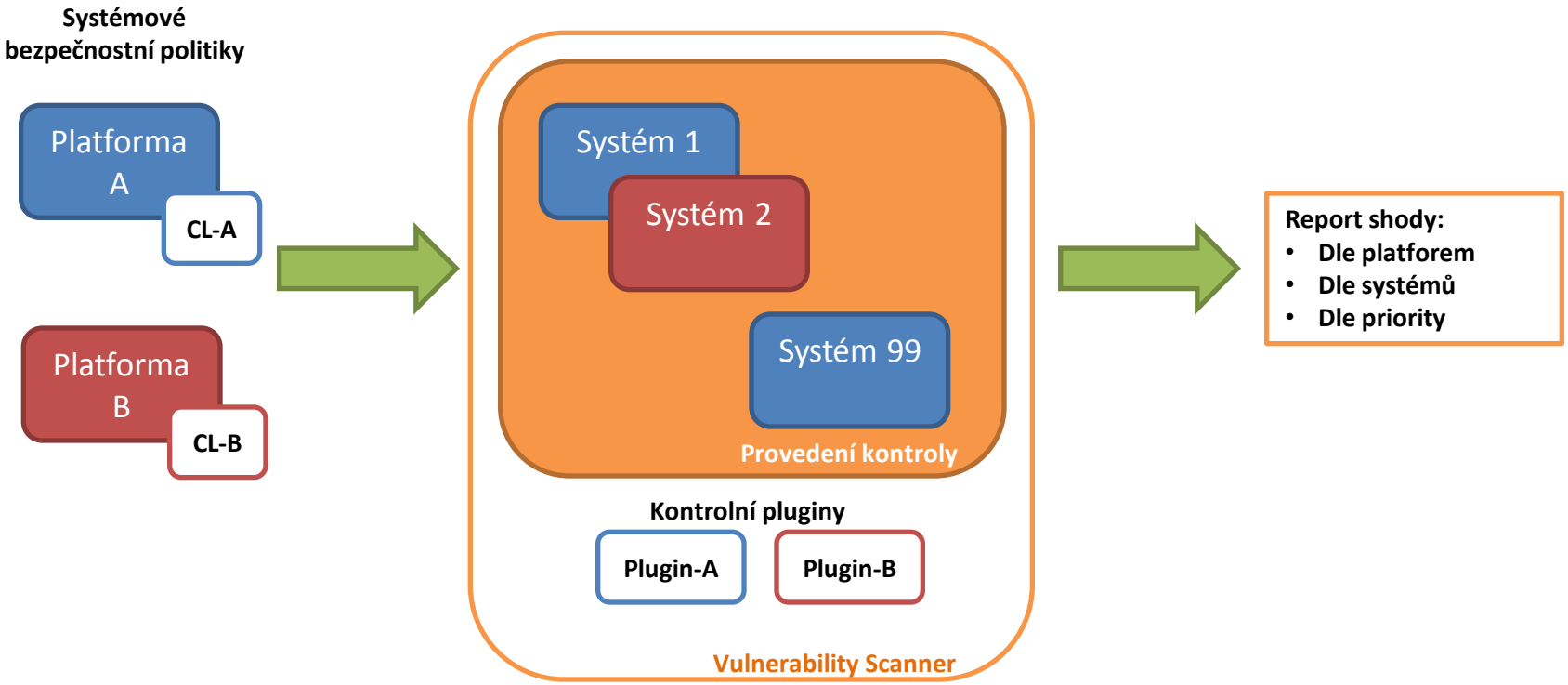
Prosazení/nastavení požadavků

Ve vazbě na jednotlivé platformy:

- Využití prvků centrální správy
- Využití připravených konfiguračních balíčků
- Využití instalačních images / masterů
- Využití specifických skriptů
- Ruční nastavení

Prosazení požadavků hardeningu a jeho ověření v rámci change managementu

Kontrola shody ve velkém



Ověření bezpečnostní politiky

- Využití checklistu – formální ověření

	A	B	C	D	E	
1	ID	Název a popis kontroly	Priorita kontroly	Aplikovatelné	Ve shodě	Zjištění/Zdůvodnění
2	**Obecné bezpečnostní požadavky**					
3	101	Aplikace posledních bezpečnostních záplat	Vysoká			
4	102	Instalace AV software	Střední			
5	103	Odinstalace nadbytečných aplikací	Střední			
6	104	Zapnutý Firewall	Vysoká			
7	**Systémová nastavení**					
8	201	Audit Policy	Vysoká			
9	202	Politiky pro Event Log	Střední			
10	203	Omezení přístupu	Střední			
11	204	Požadování silného šifrovacího klíče	Střední			

- Využití Vulnerability scanneru – technické ověření

High	ID204 Windows 7 - Zakazani nepouzivanych sluzeb (Internet Connection Sharing; nastaveni: Disabled) v4
High	ID121 Windows 7 - Vyzadovani silneho klice relace v4
High	ID120 Windows 7 - Vzdy digitalne zasifrovat nebo podepsat
High	ID119 Windows 7 - Podepisovani komunikace v4
High	ID116 Windows 7 - Minimalni zabezpeceni relace pro klienty
High	ID115 Windows 7 - Zakazani odesilani nezasifrovaneho hes
High	ID109 Windows 7 - Heslem chraneny screensaver v4
High	ID108 Windows 7 - Zakazani automatickeho prihlaseni do re
High	ID107 Windows 7 - Zakazani Autorun (pro CD) v4
High	ID106 Windows 7 - Velikosti event logu v4
High	ID105 Windows 7 - Nastaveni auditovani v4
High	ID102 Windows 7 - Politika hesel v4
High	ID111.Windows 7 - Zobrazeni banneru pri prihlasovani uziva
High	ID201.Windows 7 - Povoleni/nastaveni firewallu v5

Prehled zranitelnosti dle severity

Plugin	Plugin Name	Severity
1005061	ID805 AIX - Nastaveni Banner /etc/ssh/ banner.txt pro SSH 804	High

Hosts in Repository [redacted]:

[redacted]

Plugin	Plugin Name	Severity
1005067	ID712 AIX - Nastaveni mesg n jako defaultni pro vsechny uzivatele a profily (kontrola mesgn v /etc/csh.login) v1	High

Hosts in Repository [redacted]:

[redacted]

Plugin	Plugin Name	Severity
1005068	ID712 AIX - Nastaveni mesg n jako	High

Kde uplatnit hardening …

- Operační systémy
- Databáze
- Virtualizační SW
- Komponenty dohledů (agenti)
- Běhová prostředí / aplikační servery

Obecně, ICT komponenty s větším výskytem

Kde začít?

- Nejčastěji využívané / kritické komponenty
- Využít potenciál centrální správy / masterů

Rekapitulace

Předpoklady úspěšného hardeningu:

- Strukturované a detailní politiky (SBP)
  - Platformní pohled
- Prosazení nastavení v infrastruktuře
  - Zakotvení v change managementu
- Ověření parametrů, kontrola
  - Efektivní, opakovatelné ověření

Hardening je myšlenka, …

… která lze realizovat.

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Pavel Hejduk
ČEZ ICT Services, a. s.
pavel.hejduk@cez.cz