Konfigurační standardy

pomoc nebo otrava?

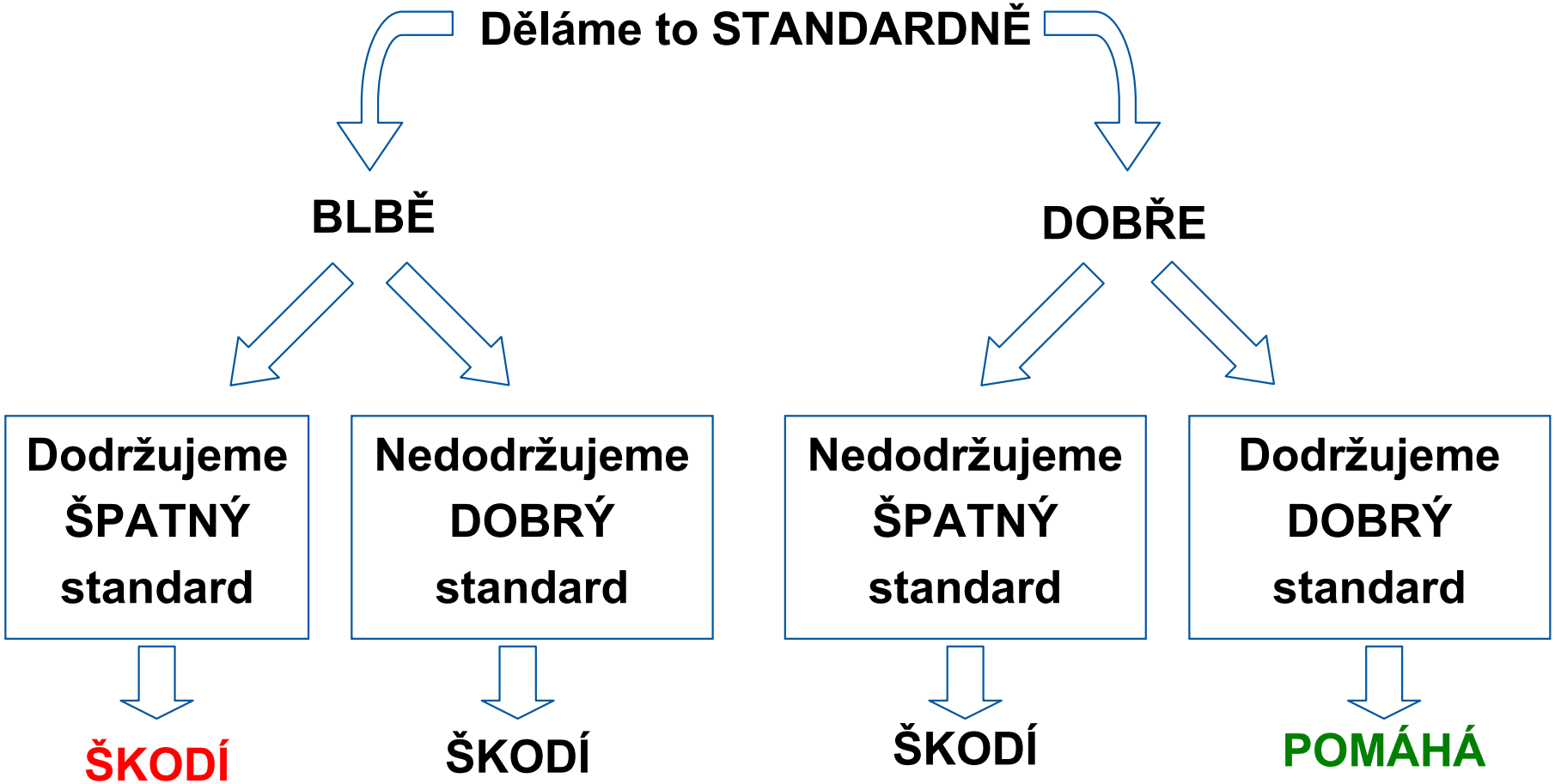
RNDr. Luboš Číž, CISA
ciz@dcit.cz
DCIT, a.s., http://www.dcit.cz

ČIMIB

AGENDA

- STANDARD – pomáhá či škodí?
- ZDROJE STANDARDŮ (kde vzít a nekrást)
- ZDROJE STANDARDŮ (kde vzít a nekrást)
- MOŽNOSTI KONTROLY KONFIGURACE
- KONFIGURAČNÍ REVIEW
- ZPŮSOB NASAZENÍ, PROVOZNÍ POŽADAVKY
- CO ZÍSKÁME?

STANDARD – pomáhá či škodí?



Standard pomáhá jen tehdy, je - li dobrý
a jsme schopni zaručit jeho dodržování !!!

ZDROJE STANDARDŮ (kde vzít a nekrást)

Kde vzít (dobré a použitelné) konfigurační standardy?

Možnosti:

Doporučení výrobců OS, DB, Aplikací – „expertní“ ale v praxi často nepoužitelné

Necháme to na dodavateli – zaručená cesta do pekel

Vymyslíme si jej sami – riziko „provozní“ slepoty nedostatečné know-how

Zpracujeme je ve spolupráci s externími konzultanty
(My dodáme znalost prostředí, oni znalost možností konfigurace)

MOŽNOSTI KONTROLY KONFIGURACE

Máme dobrý konfigurační standard, ale je implementován a DODRŽUJE SE?

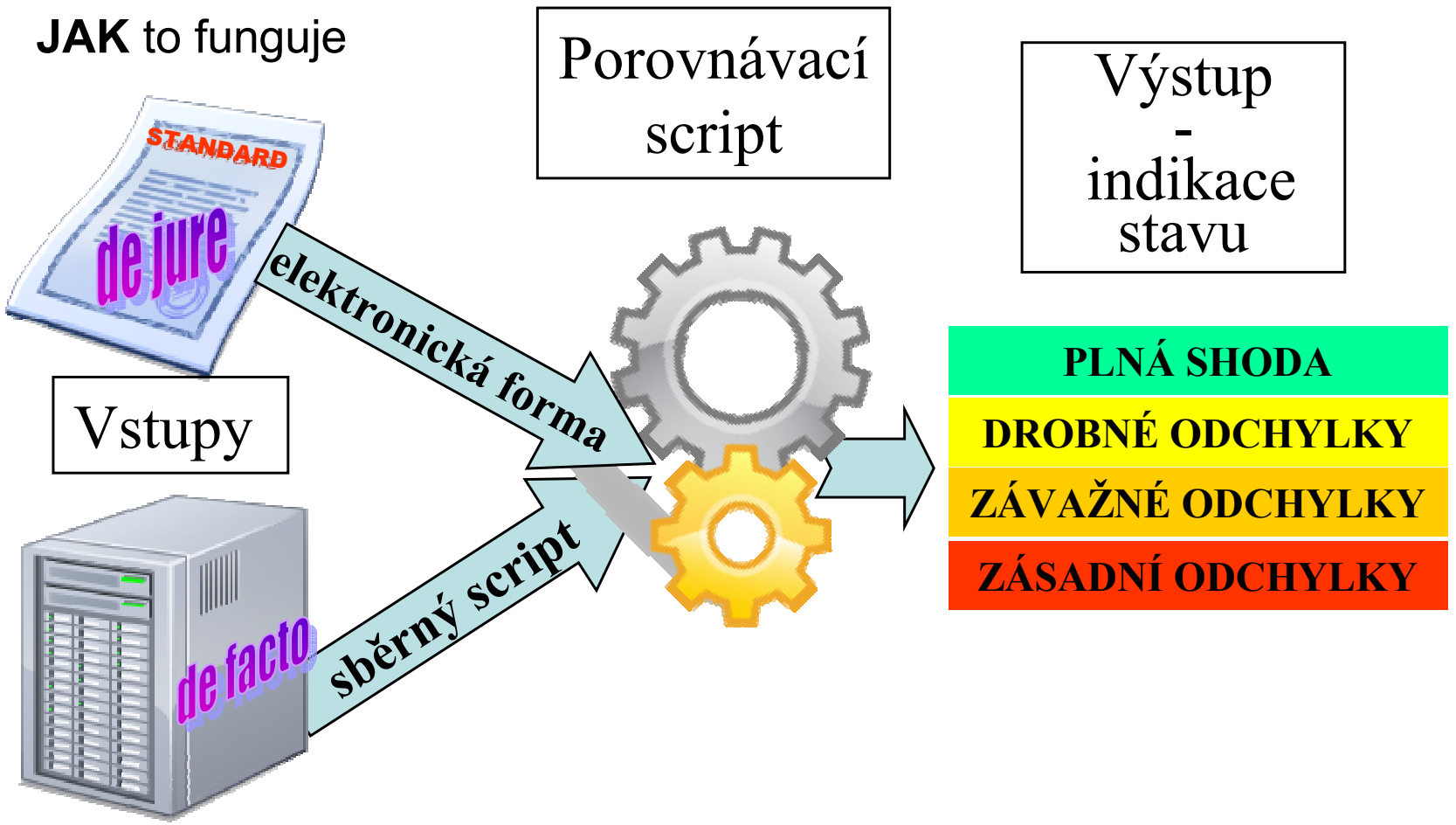
Možnosti kontroly dodržování konfiguračních standardů.

- Kontrola instalace + kontrola změn
  (změny konfiguračních parametrů nepovoleny)

- Periodická kontrola konfigurace
  (Audit OS, DB, Aplikací nebo konfigurační review)
  - Pravidelná
  - Nepravidelná

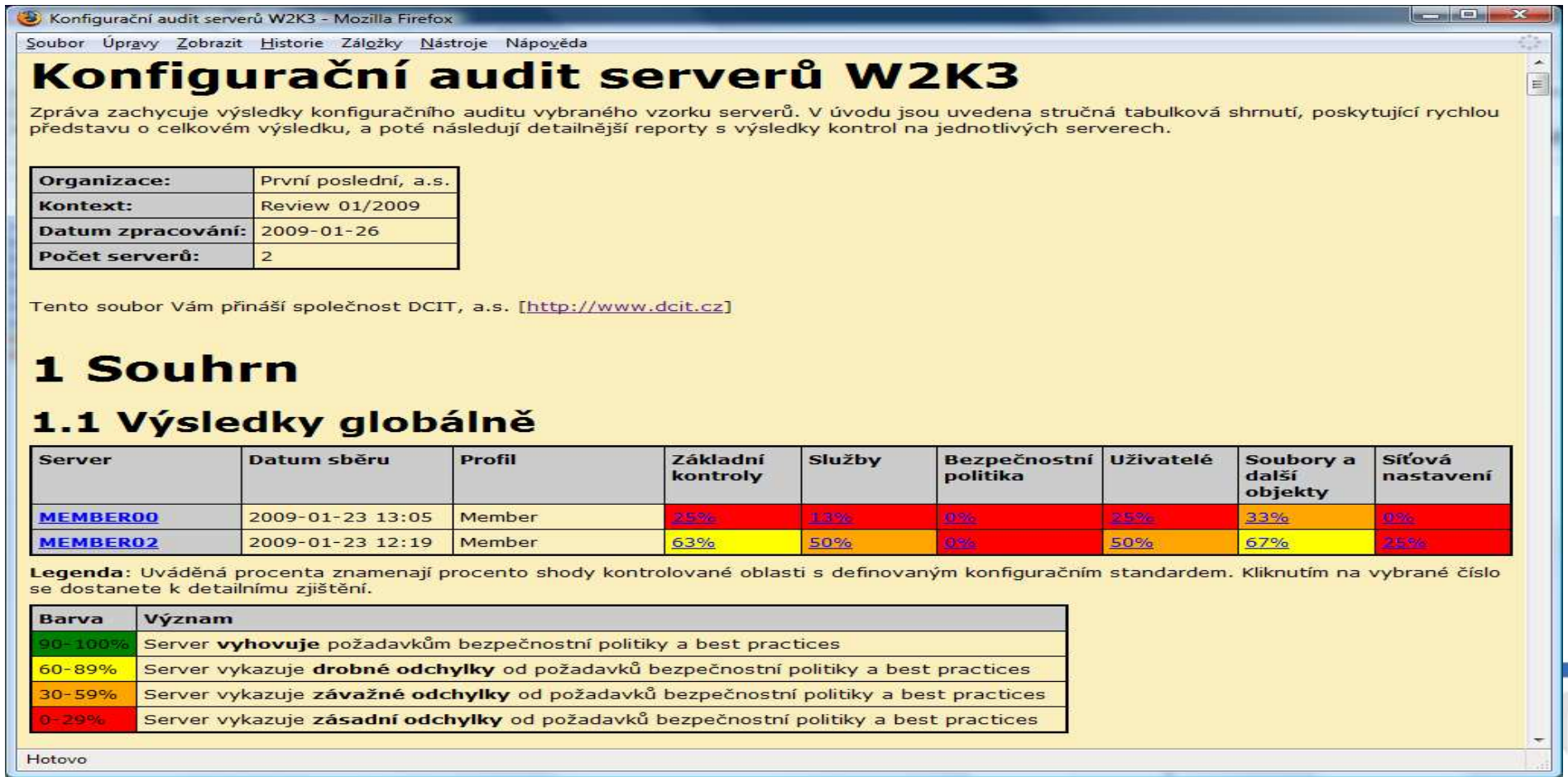
KONFIGURAČNÍ REVIEW

- **CO** to je
  Automatizovaný způsob plošné kontroly konfigurace operačních systémů a databází
- **PROČ**
  Pro ujištění se o dodržení zvoleného standadu
- **JAK** to funguje



KONFIGURAČNÍ REVIEW

- **KDY**
  Kdykoliv chcete
  (Ad hoc spouštění nebo naplánování v sheduleru
- **CO** ZÍSKÁME
  Velmi rychlý celkový přehled



Konfigurační audit serverů W2K3 - Mozilla Firefox

Soubor Úpravy Zobrazit Historie Záložky Nástroje Nápověda

Konfigurační audit serverů W2K3

Zpráva zachycuje výsledky konfiguračního auditu vybraného vzorku serverů. V úvodu jsou uvedena stručná tabulková shrnutí, poskytující rychlou představu o celkovém výsledku, a poté následují detailnější reporty s výsledky kontrol na jednotlivých serverech.

Organizace:	První poslední, a.s.
Kontext:	Review 01/2009
Datum zpracování:	2009-01-26
Počet serverů:	2

Tento soubor Vám přináší společnost DCIT, a.s. [http://www.dcit.cz]

1 Souhrn

1.1 Výsledky globálně

Server	Datum sběru	Profil	Základní kontroly	Služby	Bezpečnostní politika	Uživatelé	Soubory a další objekty	Síťová nastavení
MEMBER00	2009-01-23 13:05	Member	25%	13%	0%	25%	33%	0%
MEMBER02	2009-01-23 12:19	Member	63%	50%	0%	50%	67%	25%

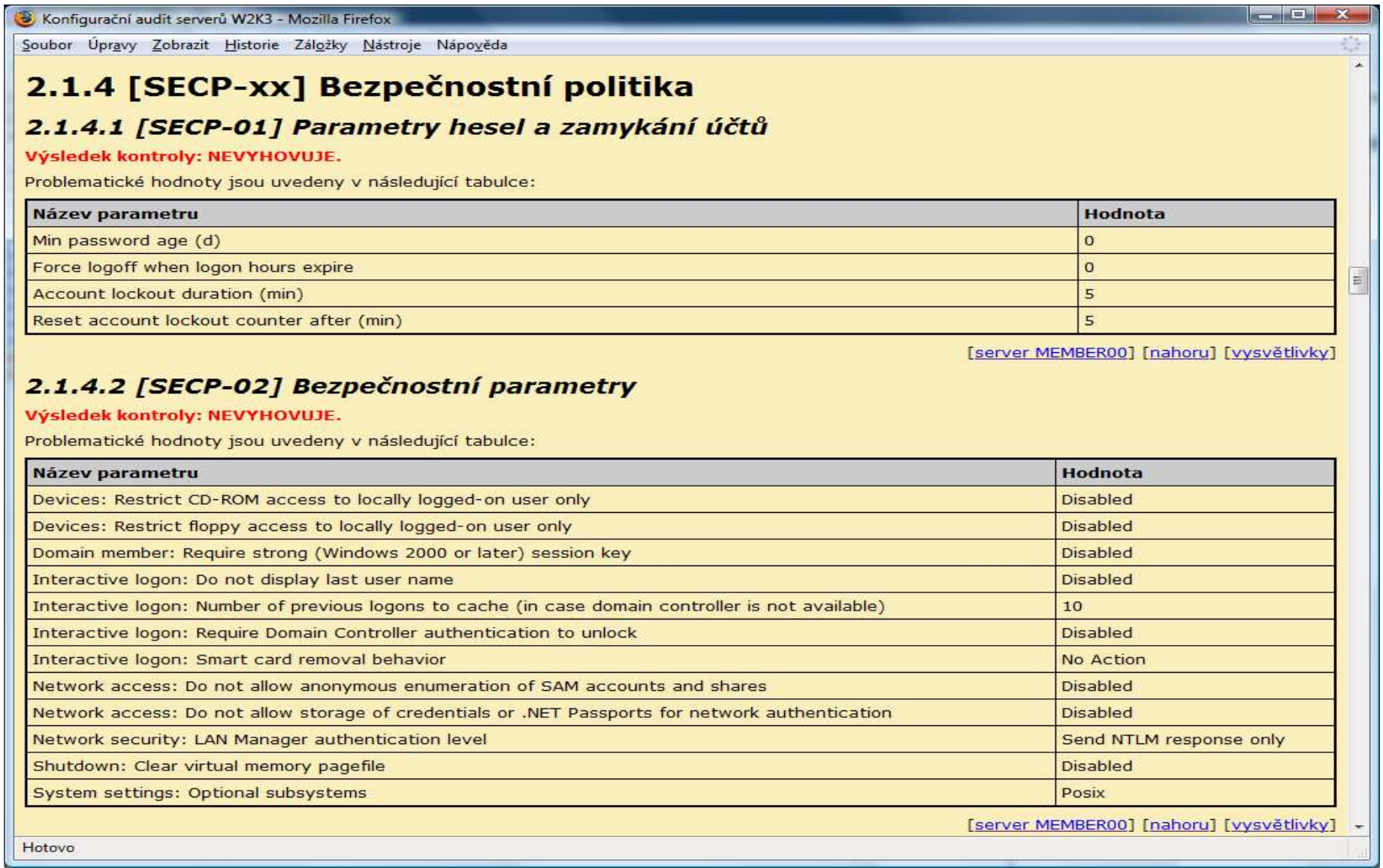
Legenda: Uváděná procenta znamenají procento shody kontrolované oblasti s definovaným konfiguračním standardem. Kliknutím na vybrané číslo se dostanete k detailnímu zjištění.

Barva	Význam
90-100%	Server **vyhovuje** požadavkům bezpečnostní politiky a best practices
60-89%	Server vykazuje **drobné odchylky** od požadavků bezpečnostní politiky a best practices
30-59%	Server vykazuje **závažné odchylky** od požadavků bezpečnostní politiky a best practices
0-29%	Server vykazuje **zásadní odchylky** od požadavků bezpečnostní politiky a best practices

Hotovo

KONFIGURAČNÍ REVIEW

- **CO** ZÍSKÁME
  I detailní přehled nevyhovujících parametrů



Konfigurační audit serverů W2K3 - Mozilla Firefox

Soubor Úpravy Zobrazit Historie Záložky Nástroje Nápověda

2.1.4 [SECP-xx] Bezpečnostní politika

2.1.4.1 [SECP-01] Parametry hesel a zamykání účtů

Výsledek kontroly: NEVYHOVUJE.

Problematické hodnoty jsou uvedeny v následující tabulce:

Název parametru	Hodnota
Min password age (d)	0
Force logoff when logon hours expire	0
Account lockout duration (min)	5
Reset account lockout counter after (min)	5

[server MEMBER00] [nahoru] [vysvětlivky]

2.1.4.2 [SECP-02] Bezpečnostní parametry

Výsledek kontroly: NEVYHOVUJE.

Problematické hodnoty jsou uvedeny v následující tabulce:

Název parametru	Hodnota
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Disabled
Domain member: Require strong (Windows 2000 or later) session key	Disabled
Interactive logon: Do not display last user name	Disabled
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10
Interactive logon: Require Domain Controller authentication to unlock	Disabled
Interactive logon: Smart card removal behavior	No Action
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled
Network security: LAN Manager authentication level	Send NTLM response only
Shutdown: Clear virtual memory pagefile	Disabled
System settings: Optional subsystems	Posix

[server MEMBER00] [nahoru] [vysvětlivky]

Hotovo

KONFIGURAČNÍ REVIEW

- **CO** ZÍSKÁME
  Velmi rychlý celkový přehled
  Detailní přehled nevyhovujících parametrů
  Přehled o zlepšování/zhoršování stavu při získání časové řady
- **PRO** jaké platformy je dostupný
  Operační systémy:
  - Windows server W2K3
  - Windows server 2008
  - AIX
  - HP UX
  - SUN Solaris

  Databáze
  - ORACLE 7i a vyšší
  - MS SQL2000 a vyšší

ČIMIB ZPŮSOB NASAZENÍ, PROVOZNÍ POŽADAVKY

- 1. KROK
  - Odsouhlasení konfiguračních standardů a jejich úprava do tabulkového (XML) tvaru
- 2. KROK
  - Distribuce sběrných scriptů na dotčené stroje (cca 1 MB)
- 3. KROK
  - Sběr dat (Spuštění scriptů)
    (ad hoc nebo schedulerem)
    cca 15-30 min, max 10 MB dat (komprimovaně)
- 4. KROK
  Zpracování dat – porovnávací script
- 5. KROK
  Výstupní report – html soubor s **přehledem nastavení vybraných položek**, které jsou z hlediska konfiguračního etalonu podstatné a/nebo jsou v rozporu. **Obsah může být upraven dle potřeby**

Porovnání serverů v organizaci

1 Souhrn

1.1 Výsledky globálně

Server	Datum sběru	Profil	Základní kontroly	Parametry a nastavení DB	DB uživatelé a role	DB privilegia	DB objekty
Server0001	09.10.2008 15:28	Ora10g (basic)	50%	33%	0%	25%	60%
Server0002	09.10.2008 15:28	Ora10g (basic)	50%	33%	40%	25%	80%
Server0003	09.10.2008 15:27	Ora10g (basic)	50%	67%	0%	25%	80%
Server0004	09.10.2008 15:29	Ora10g (basic)	50%	67%	40%	25%	80%
server0005	09.10.2008 16:10	Ora10g (basic)	50%	33%	20%	25%	100%
server0006	09.10.2008 16:11	Ora10g (basic)	50%	33%	40%	25%	80%
server0007	09.10.2008 16:13	Ora10g (basic)	50%	33%	40%	25%	80%
server0008	09.10.2008 16:14	Ora10g (basic)	50%	33%	40%	25%	80%
server0009	09.10.2008 16:16	Ora10g (basic)	50%	33%	40%	25%	80%
server0010	09.10.2008 16:17	Ora10g (basic)	50%	33%	40%	25%	80%

Legenda: Uváděná procenta znamenají míru shody kontrolované oblasti s definovaným konfiguračním standardem. Kliknutím na vybrané číslo se

Hotovo

Porovnání serveru v čase

1 Souhrn

1.1 Výsledky globálně

Server	Datum sběru	Profil	Základní kontroly	Služby	Bezpečnostní politika	Uživatelé	Soubory a další objekty	Síťová nastavení
WXPW3	2008-07-02 23:40	Stdalone	25%	50%	0%	25%	100%	100%
WXPW3	2008-07-02 23:45	Stdalone	25%	50%	0%	25%	100%	50%
WXPW3	2008-07-03 08:39	Stdalone	25%	50%	0%	25%	100%	50%

Legenda: Uváděná procenta znamenají míru shody kontrolované oblasti s definovaným konfiguračním standardem. Kliknutím na vybrané číslo se dostanete k detailnímu zjištění.

Barva	Význam
90-100%	Server **vyhovuje** požadavkům bezpečnostní politiky a best practices
60-89%	Server vykazuje **drobné odchylky** od požadavků bezpečnostní politiky a best practices
30-59%	Server vykazuje **závažné odchylky** od požadavků bezpečnostní politiky a best practices
0-29%	Server vykazuje **zásadní odchylky** od požadavků bezpečnostní politiky a best practices

1.2 Výsledky podrobněji

Server	Total	Základní kontroly								Služby						Bezpečnostní politika					Uživatelé				Soubory a další objekty			Síťová nastavení			
		01	02	03	04	05	06	07	08	01	02	03	04	05	06	01	02	03	04	05	01	02	03	04	01	02	03	01	02	03	04
WXPW3	47%	fail	fail	fail	ok	fail	fail	fail	ok	fail	fail	fail	ok	ok	ok	fail	fail	fail	fail	fail	fail	fail	fail	ok	ok	ok	ok	ok	ok	ok	ok
WXPW3	41%	fail	fail	fail	ok	fail	fail	fail	ok	fail	fail	fail	ok	ok	ok	fail	fail	fail	fail	fail	fail	fail	fail	ok	ok	ok	ok	fail	fail	ok	ok
WXPW3	41%	fail	fail	fail	ok	fail	fail	fail	ok	fail	fail	fail	ok	ok	ok	fail	fail	fail	fail	fail	fail	fail	fail	ok	ok	ok	ok	fail	fail	ok	ok

Legenda: V případě kontrol, které zjistily nedostatek, se kliknutím na "fail" dostanete k detailnímu zjištění. Tooltip přitom uvádí detailnější specifikaci příslušné kapitoly.

Děkuji za pozornost

- Podrobnější informace a vzory výstupních zpráv za různé platformy zašleme na vyžádání e-mailem

- Kontakt

  info@dcit.cz

  ciz@dcit.cz