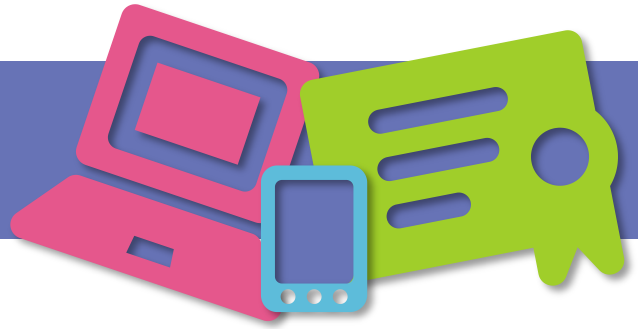
SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Když logy nestačí

Libor Kovář, Peter Jankovský

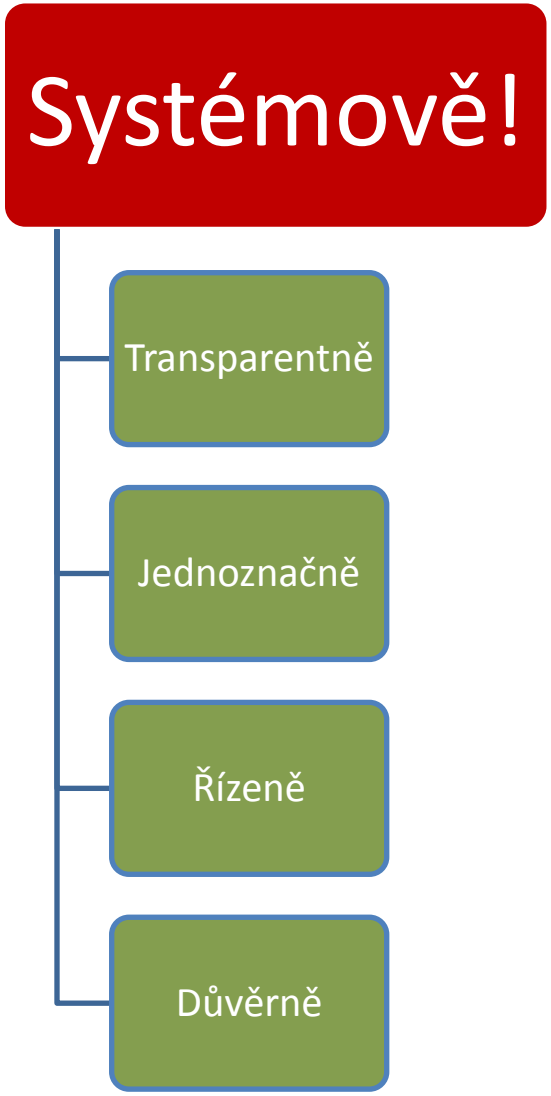
ČEZ, AXENTA

OSNOVA

- **Vstupní impulz**
  - Koho a Jak?
- **Technologie**
  - Balabit Shell Control Box
- **SPVŘ + režim**
- **Využití SCB v prostředí SPVŘ**
  - kontrola adminů
  - kontrola dodavatele
  - důkazní břemeno
  - udržení know-how

Impulz - SPVŘ

- **Koho monitorovat?**
  - Privilegovaní uživatelé
- **Jak monitorovat - I.**
  - Log data / SIEM eventy
- **Jak monitorovat - II.**
  - Recording činností/ Auditing
  - **Systémový přístup!**



BalaBit - Shell Control Box

Transparentně | Jednoznačně | Řízeně | Důvěrně

Shell Control Box – RDP, ICA, SSH, VNC, TELNET, HTTP/S

- Bez agenta
- Man-In-The-Middle
- Network Layer 2/3

- TSA
- HASH
- WORM

- Kanály
- Časová okna
- Uživatelské skupiny
- 4 oči/2 hlavy
- Alerty

- AAA
- Šifrování
- Audit Player
- Indexer / OCR

Informační systém SPVŘ

SPVŘ – systém pro podporu výstavby bloku 3,4 ETE

Systém umístěn ve dvou lokalitách

- **<u>Základní bezpečnostní premisy:</u>**
- systém SPVŘ je zcela izolovaný
- přístup do systému SPVŘ je řízený
- přístup k datům (aktivům) je řízený
- práce systému SPVŘ je auditovaná
- systém SPVŘ neumožňuje práci pod generickými účty
- systém SPVŘ autorizuje přístup ke všem datům
- systém SPVŘ zaznamenává systémové události

Pravidla pro práci v SPVŘ

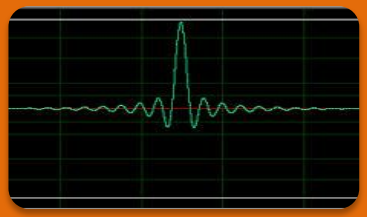
1. Co není povoleno (odpovědnou osobou, dokumentací, …), je zakázáno!!!

2. Vše je pod dohledem a pouze s doprovodem!!!

Správci systému ani **dodavatelé** nesmí

- přistupovat k informacím výběrového řízení
- přistupovat k systémům a konfiguraci bezpečnostních komponent.

SCB v prostředí SPVŘ

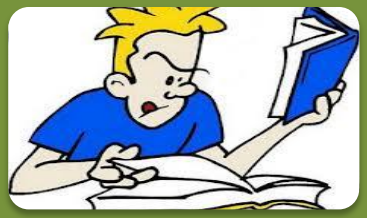


Prvotní impuls

- kontrola administrátorů
- kontrola dodavatelů

Dokonalý provozní deník

- vše co administrátor vykoná je zaznamenáno ve formě videa a lze to kdykoli přehrát



Revize postupů

- Incident Response
- Change management

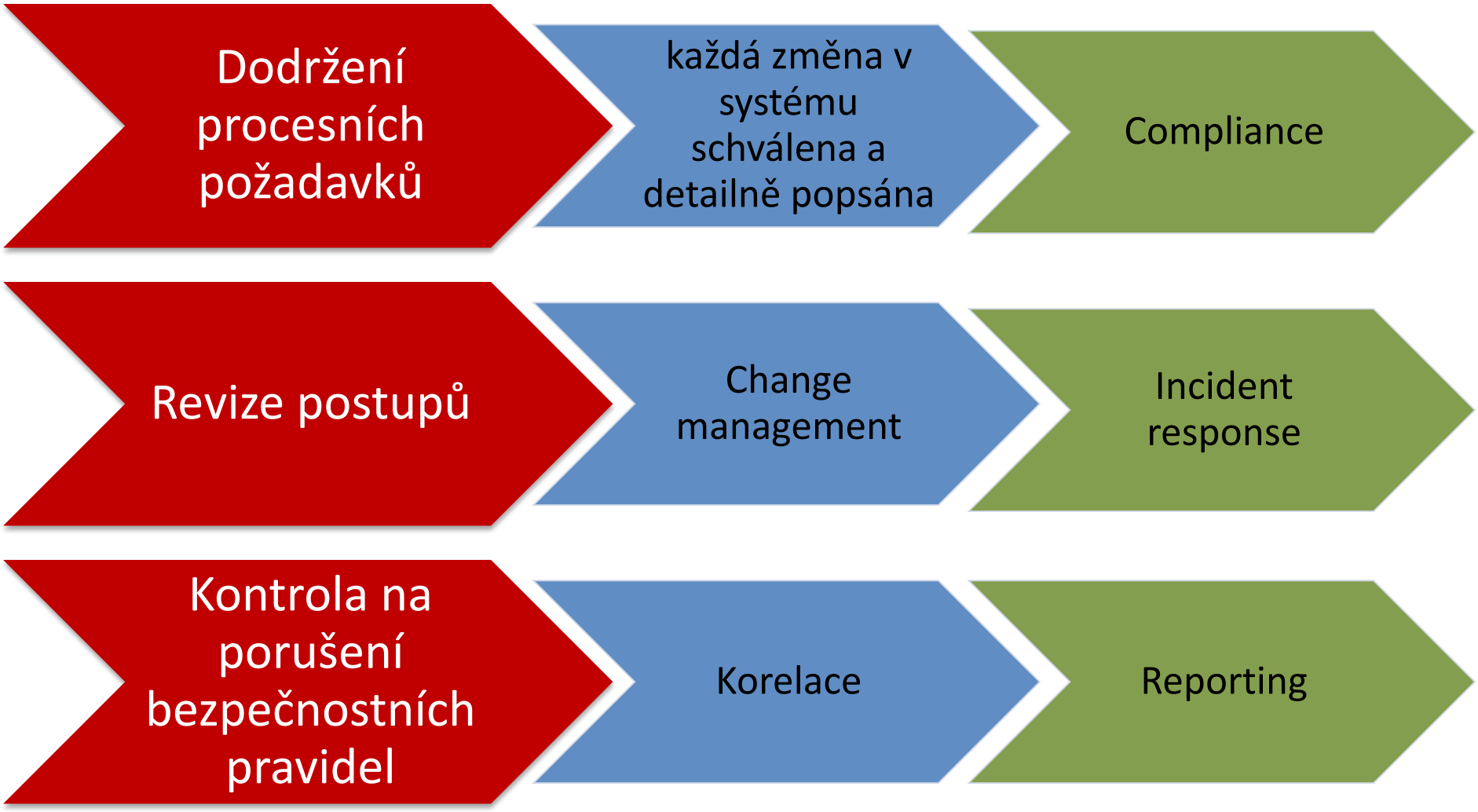
Kontrola principem 4 očí

- Vynutitelnost kontroly
- Vynutitelnost aktivit

Kontrola činnosti administrátorů

Každodenní namátková činnost BS	anomálie
Kontrola dodržení schválených change-managementů	neshody
Kontrola dodržení procesů a dokumentace	odhalená ukrytá hesla
Vyhledávání / zpětná vazba/ při chybách a opravách administrátorů	recovery

Kontrola činnosti dodavatele



Udržení know-how

Knowledge Base

- Zpětné dohledání změn v konfiguracích – i špatně zadaná hesla
- Při činnosti dodavatele zpětné přehrání jeho kroků a následná možná replikace
- Možnost se v postupu vrátit zpět
- Jednodušší dohledání problému v logách

Důkazní břemeno

- Nedodržení schválených postupů je **on-line detekováno**
- Při incidentu je dohledání činnosti **admina** v real-time bodě:
  - Nestihne utéci, ani zahladit stopy.
  - Zabránění vyhazovu administrátora při porušení bezpečnosti v důsledku jeho omylu.
- Okamžité a nezpochybňované řešení neshod mezi **administrátory**
- Kontrola historie činnosti **admina** – **waste time**
- Kontrola konspirace - **nemožnost ukrýt chybnou/nekalou činnost**

Závěr

V **extrémně zahardenovaném prostředí** je náročnější ladění v případě neočekávaných chyb

V případě potřeby zabezpečení auditu administrátorů lepší nástroj není

Pro systémy na bezpečnostní úrovni SPVŘ lze jen doporučit

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Ing. Libor Kovář, ČEZ, a.s.
libor.kovar@cez.cz
Ing. Peter Jankovský, AXENTA a.s.
jankovsky@axenta.cz