Security Management

Radovan Semančík

Čo je to bezpečnosť?

Čo je to bezpečnosť?

Bezpečnosť je proces

A process cannot be understood by stopping it. Understanding must move with the flow of the process, must join it and flow with it.

-- First Law of Mentat

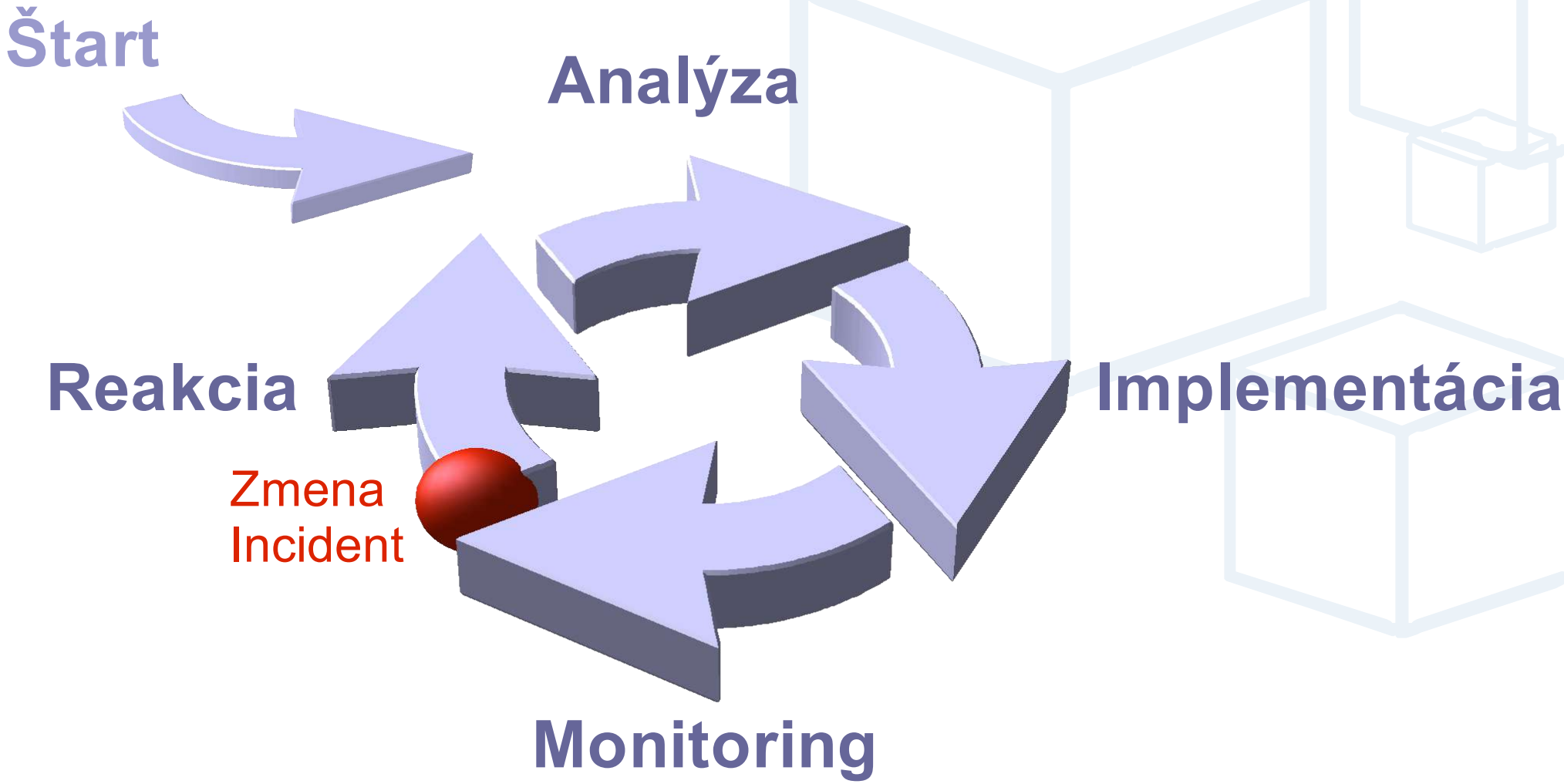
BGS
Business Global Systems

Čo nie je bezpečnosť?

- Firewall nie je bezpečnosť
- “Bezpečnostný projekt” nie je bezpečnosť
- “Patchovanie” nie je bezpečnosť

- Bezpečnosť nie je produkt, projekt, riešenie, ...
- Bezpečnosť nie je statická, ale dynamická

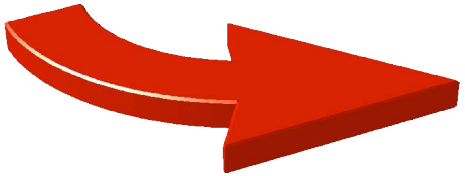
Bezpečnostný manažment



BGS
Business Global Systems

“Bezpečnostný projekt”

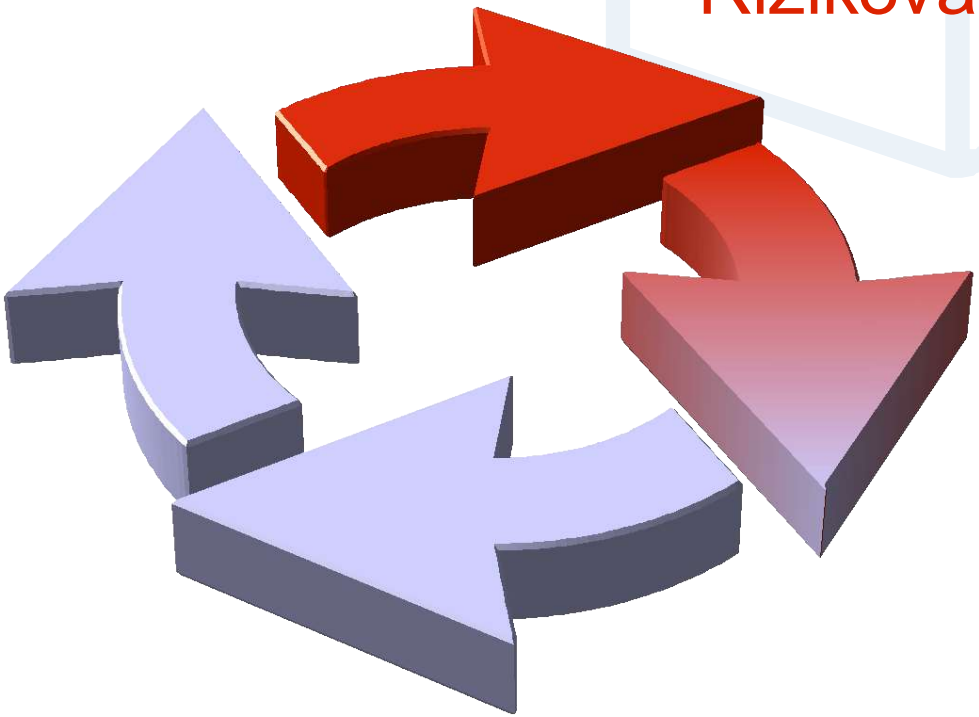
Príprava projektu



Bezpečnostná politika, požiadavky

Riziková analýza

Návrh opatrení



BGS
Business Global Systems

Bezpečnostný proces

Príprava projektu

Bezpečnostná politika, požiadavky

Riziková analýza

Návrh opatrení

Implementácia opatrení

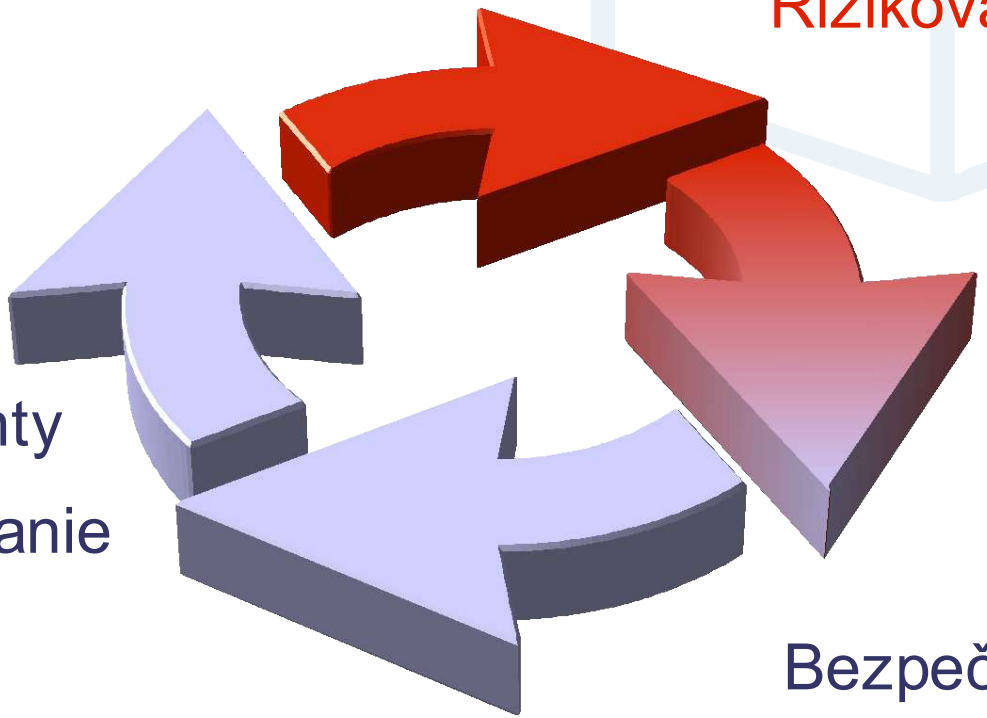
Bezpečnostný audit

Pevádzka a monitoring

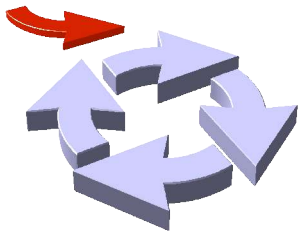
Revízie

Reakcia na icidenty

Zmenové konanie



BGS
Business Global Systems

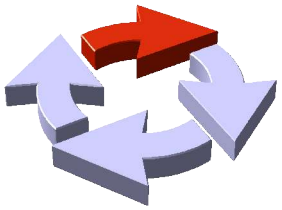


Príprava projektu

- Vytvorenie projektového tímu
  - Vyšší manažment: presadenie výsledkov, podpora
  - Bezpečnostný správca
  - Systémový správca, správca siete, ...
- Určenie rozsahu a metodiky projektu
  - Krátka a rýchla analýza
- Informovanosť

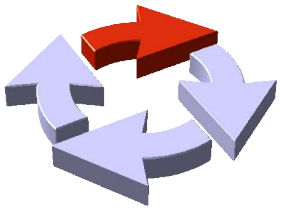
“Security Officer”

- Administrátor
  - Uľahčovať život
  - Chod systémov
  - Nehody, chyby
  - Len IT
  - ...
- Security Officer
  - Komplikovať život
  - Bezpečnosť systémov
  - Útočník (+ nehody, chyby)
  - Nie len IT
  - ...



Bezpečnostná politika

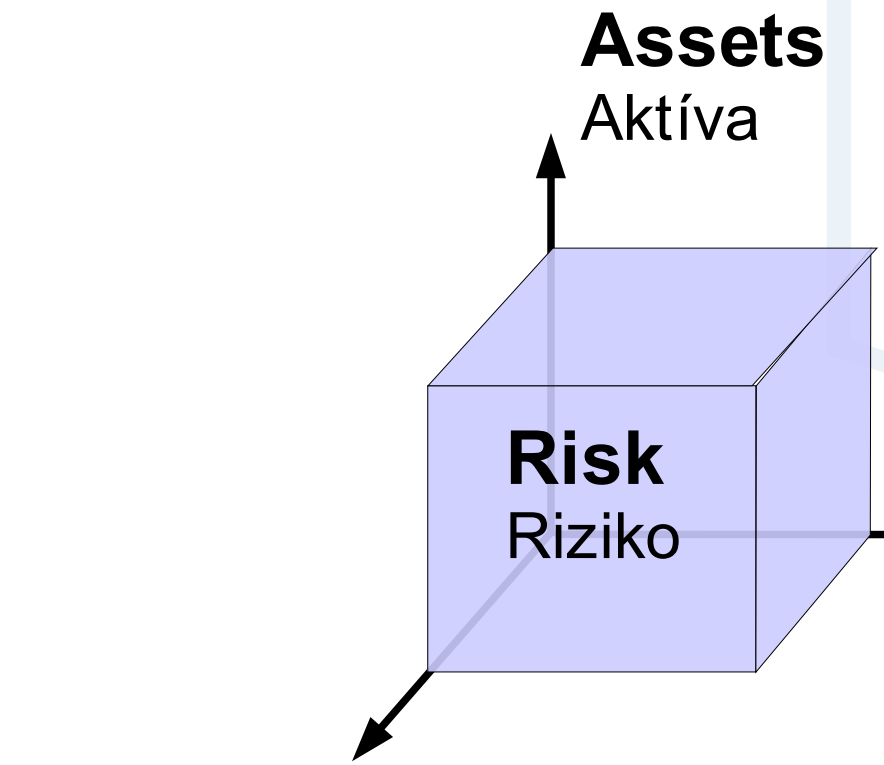
- Vyjadrenie zámeru a cieľov
  - Jasná podpora top manažmentu
  - Bezpečnosť je priorita
- Obsah dokumentu
  - Konrétne pravidlá (malé organizácie)
  - Rámec pre smernice (väčšie organizácie)
- Nemala by sa obmedzovať len na IT



Riziková analýza

- Zhodnotenie úrovne rizika
- Druhy “analýzy”:
  - **Security Assessment:** neformálna
  - **Risk Analysis:** formálna, použitý model
  - **Audit:** formálna, potvrdenie stavu

Riziková analýza – model

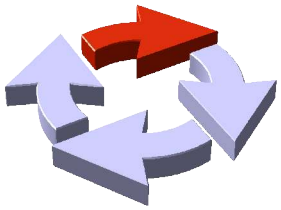


- Databáza zákazníkov
- Web server
- Chod výroby

- Hacker
- Zlodej
- Požiar

- Diera vo firewalle
- Okno bez mreží
- Nefunkčný hasiaci prístroj

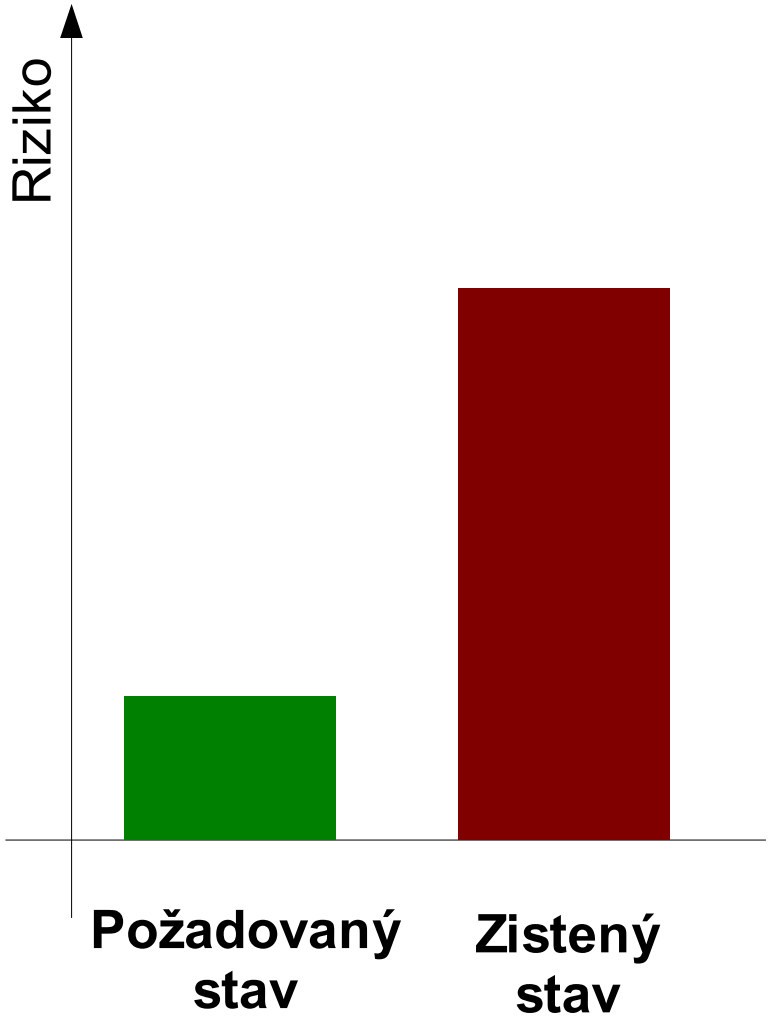
BGS
Business Global Systems

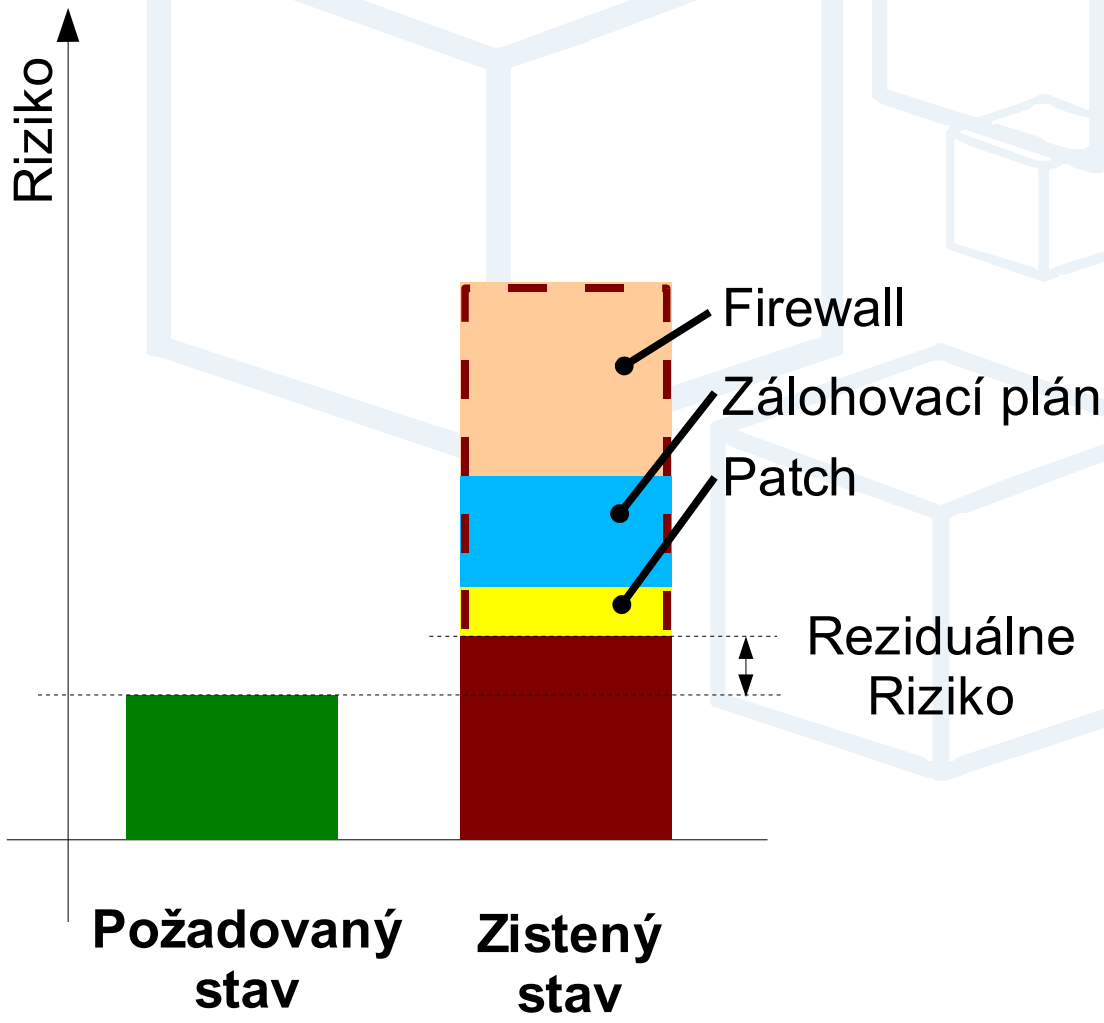


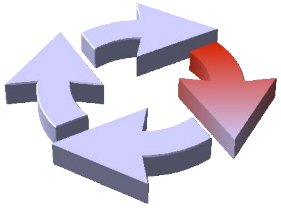
Riziková analýza

- Model
  - Kvantitatívny ($$$)
  - Kvalitatívny (“málo”, “mierne”, “veľa”)
- Vedenie analýzy
  - Automatizovaný nástroj (RiskPac, CRAMM, ...)
  - Experné zhodnotenie
- Výsledok
  - Zhodnotenie rizík v určitých oblastiach
  - CIA, Fyzická-logická-antivírová-zálohovanie-...

Návrh opatrení

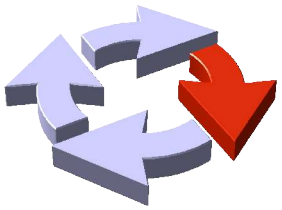






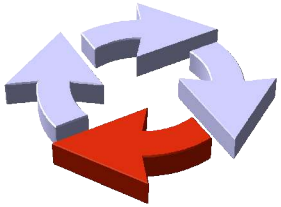
Návrh opatrení

- Návrh bezpečnostných opatrení
  - Krátkodobá varianta (Málo $$$, rýchlo)
  - Dlhodobá varianta (Systematické riešenie)
- Návrh procesov bezpečnostného manažmentu
  - Monitorovanie, reakcia na incidenty
  - Revízie, pravidelné činnosti
  - Havrijné plánovanie
  - Zachovanie kontinuity



Implementácia opatrení

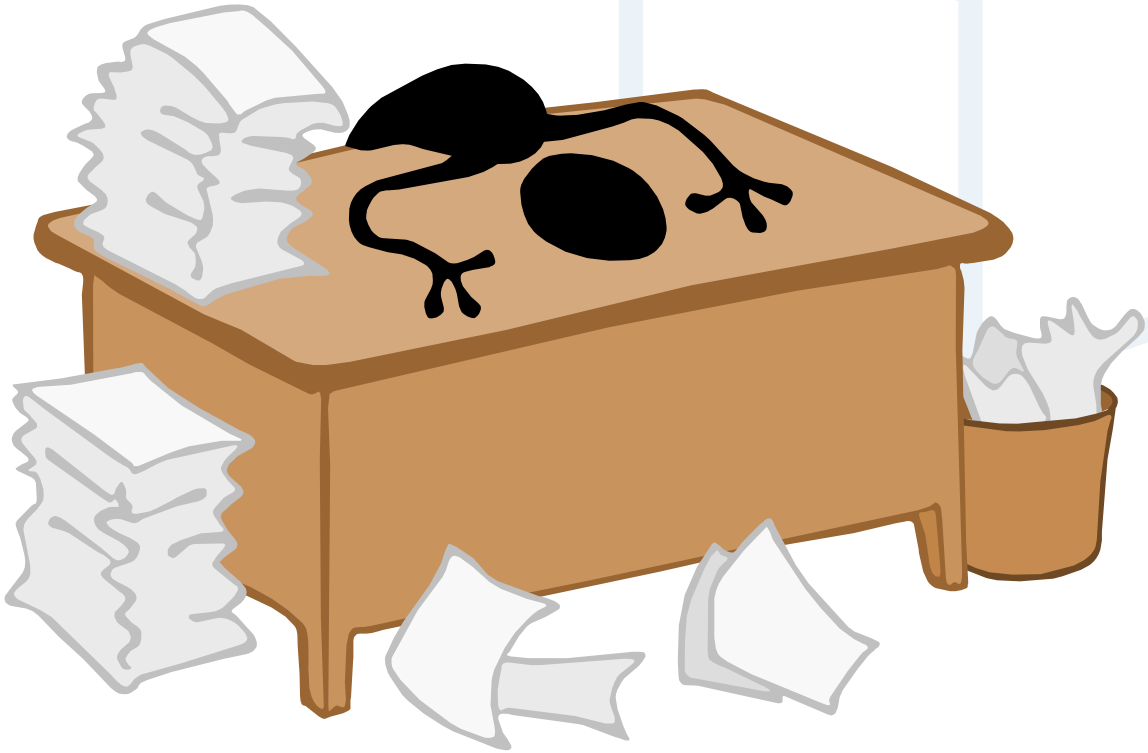
- Implementovať to, čo bolo navrhnuté
- Samostatné projekty pre čiastkové úlohy
  - Autentifikácia, SSO
  - Firewalling
  - Monitoring systémy, zbieranie logov
  - Zavádzanie procesov a procedúr
  - ...



Bezpečnostný audit

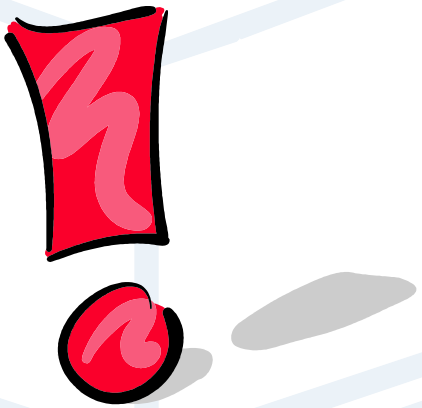
- Potvrdenie, že opatrenia boli implemetované správne
- Formalizovaná metodológia
- CISA – Certified Information Systems Auditor
  - ISACA – Information Systems Audit and Control Assoc.

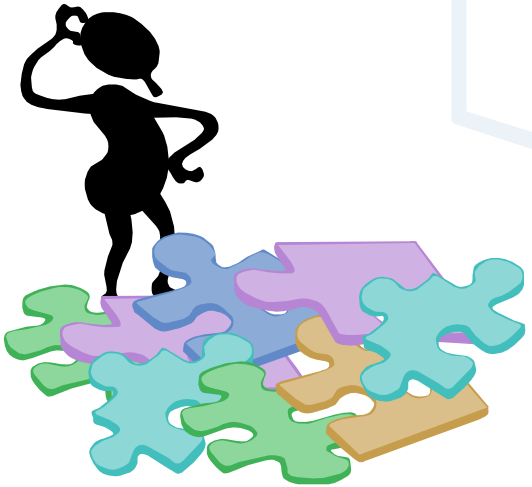
Prevádzka a monitoring



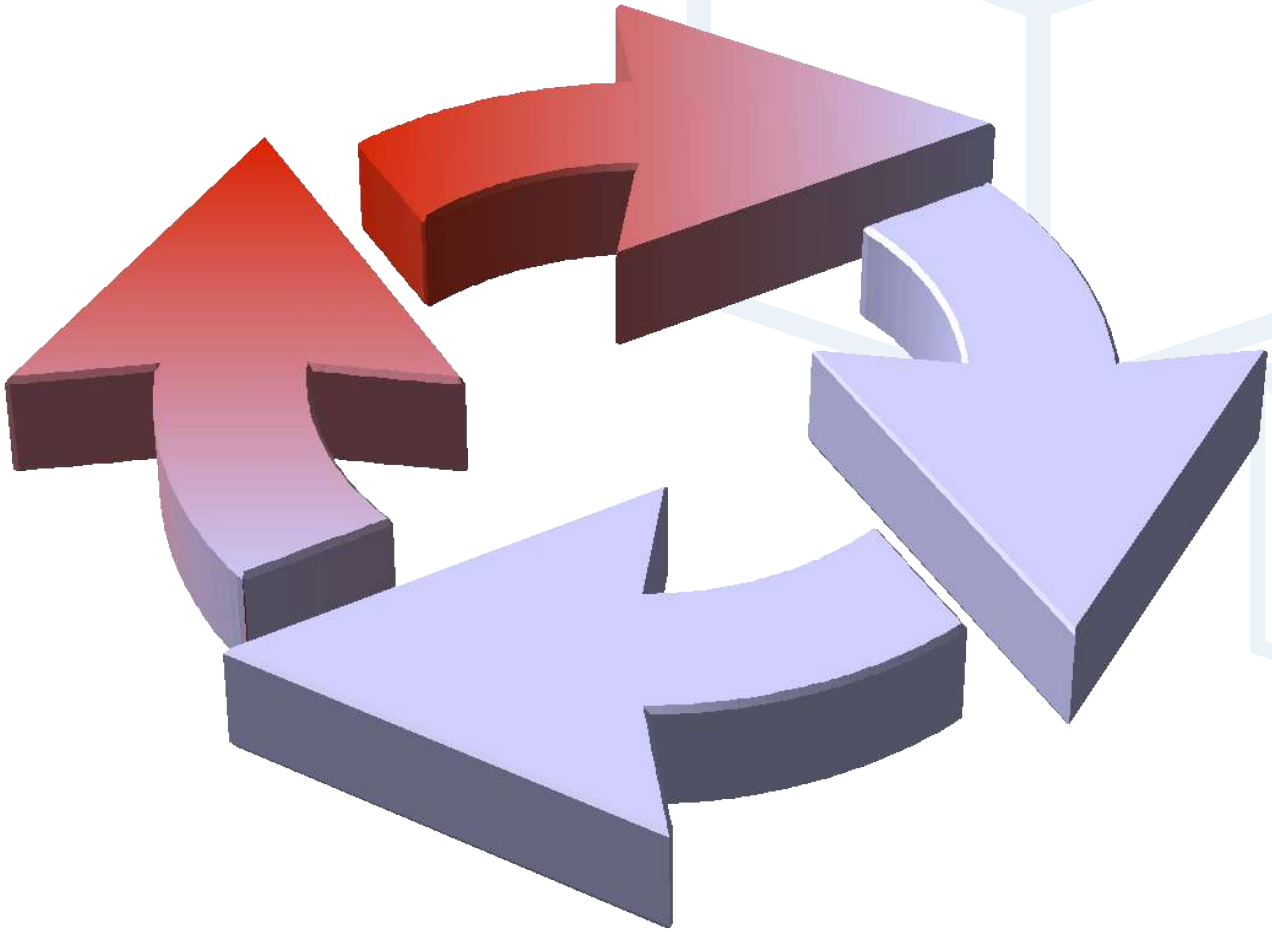
Incident

Reakcia





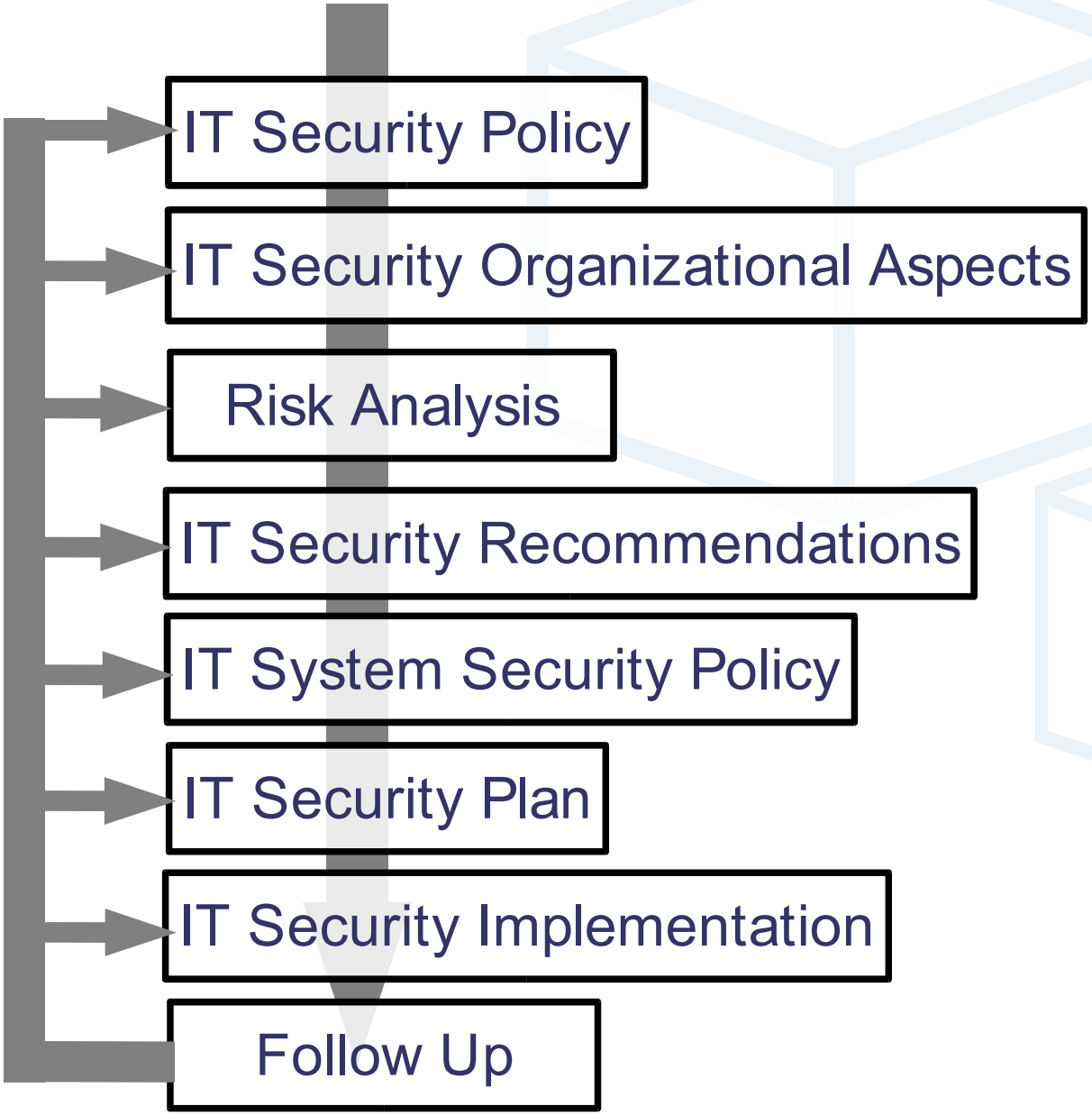
Reakcia



Zákony a normy

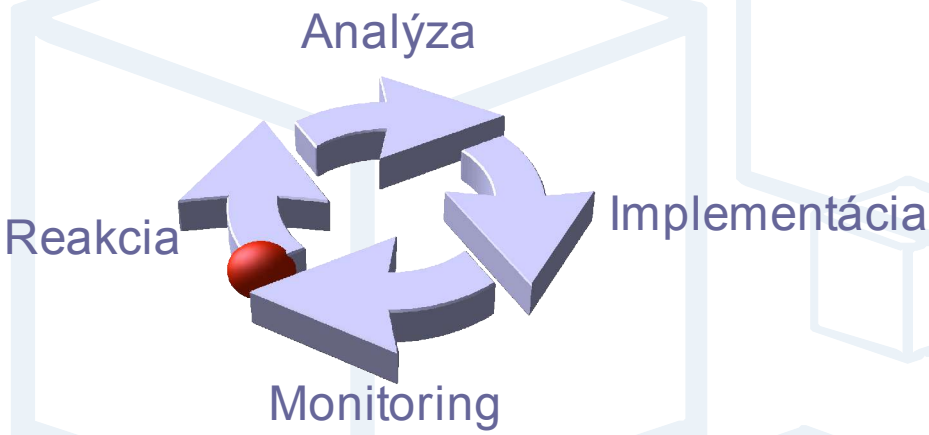
- Ochrana osobných údajov (428/2002)
  - Vytvorený “bezpečnostný projekt”
- Ochrana utajovaných skutočností (241/2001)
  - Zákon a vyhlášky
  - Rôzne požiadavky pre rôzne úrovne
- ISO 17799 (BS 7799): IT Security Management
- ISO TR 13335: Guidelines for IT Security
- ISO 15408: Common Criteria

ISO TR 13335



Záver

- Bezpečnosť je proces
- Bezpečnosť je **proces**
- Bezpečnosť je *proces*



- Základ: Bezpečnostná politika
- Aspoň základná riziková analýza (1 stránka A4)
- Implementácia procesov:
  - Zálohovanie, monitoring logov, revízie konfigurácií, ...
- Monitoring a reakcia

Záver

- Bezpečnosť je reakčný systém
  - Reaguje na (nepredvídané) incidenty

The road of life can only reveal itself as it is traveled; each turn in the road reveals a surprise. Man's future is hidden.

-- Anonymous

Questions?

Bonus Track:
Bezpečnostné povery a mýty

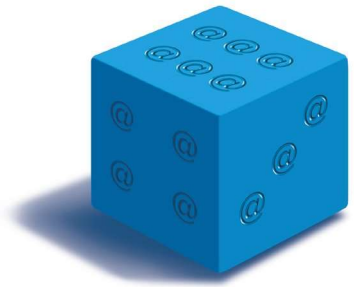
Buzzword Dictionary – Vol. II:
Security Buzzwords

Thank you ...

Ing. Radovan Semančík

Business Global Systems, a.s.
Pluhová 2
83248 Bratislava

semancik@bgs.sk



BGS
Business Global Systems