SECURITY 2011

19. ročník konference o bezpečnost v ICT

Nasazení bezpečnostního monitoringu v praxi

Jan Svoboda

AEC

Obsah

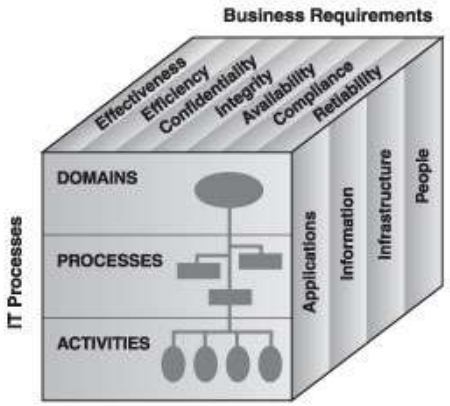
- Kde začít
- Jak definovat požadavky na řešení
- Jak vybrat to správné řešení

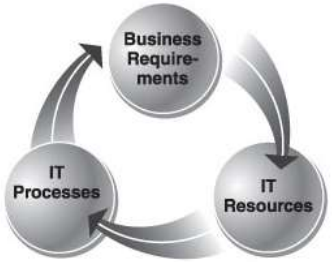
Kde a čím začít

- Identifikace základních potřeb bezpečnostního monitoringu
  - Soulad s mezinárodními standardy
    - PCI DSS
    - ISO 27002
    - SOX
  - Soulad se zákonem daným opatřením
    - Doba archivace logovaných událostí
    - Přístup k citlivým údajům
  - Soulad s group policy
    - Požadavky na bezpečnostní monitoring stanovené mateřskou společností
    - Požadavky interního auditu
  - Vlastní potřeby kontroly a včasné reakce
    - Provozování kritických systémů
    - Kontrola segmentu IT (outsourcing)

Kde a čím začít

- Vytvoření a aplikace procesních opatření
  - Definování potřebných rolí
    - Bezpečnostní manager
    - Administrator
    - Operátor
    - a další……
  - Definice odpovědností
    - Administrace
    - Řízení incidentů/změn
    - Eskalace
    - Schvalování
  - Definice a následné zavedení jednotlivých procesů
    - Incident management
    - Change management
    - SLA





Kde a čím začít

- Identifikovat zdroje bezpečnostních událostí
  - Definovat zařízení/aplikace v souladu se základními potřebami
    - Identifikace příslušných systémů infrastruktury
    - Identifikace příslušných aplikací
  - Definovat kritická zařízení infrastruktury
    - Identifikace kritických zařízení
    - Identifikace dopadů bezpečnostních incidentů na kritických zařízeních infrastruktury
  - Definovat kritické aplikace
    - Interní HR systémy
    - Aplikace publikované do internetu
    - Aplikace s možným dopadem na finance

Jak definovat požadavky na řešení

- Potřebný detail logování
  - Soulad se základními potřebami
    - Předepsaný level logovaných událostí
    - Identifikace typu událostí (user,system..)
    - Vytvoření assetu pro každé zařízení
  - Identifikace unikátních incidentů
    - Identifikace zdroje/ů událostí
    - Identifikace konkrétních událostí

Jak definovat požadavky na řešení

- Objem zpracovávaných událostí
  - Definovat počty událostí
    - Identifikovat počty událostí (nejlépe za sekundu)
    - Zapnutí logování
  - Definovat objem událostí za požadované období
    - Spočítat objem logovaných událostí v souladu se základními potřebami
    - Zapnutí logování

Jak definovat požadavky na řešení

- Základní nastavení bezpečnostních incidentů
  - Definovat základní nastavení v souladu s potřebami
    - Identifikovat jednotlivé události případně typy událostí
    - Stanovit base lines pro některé typy událostí
    - Definice interakce (email, snmp …….)
  - Definice unikátních bezpečnostních incidentů
    - Identifikovat jednotlivé události případně typy událostí
    - Stanovit base lines pro některé typy událostí
    - V případě nestandardních zařízení shromáždění vzorového záznamu logovaných událostí

Jak definovat požadavky na řešení

- Základní požadavky na výstup/reporty
  - Definovat požadavky na výstupy v souladu s potřebami
  - Definovat požadavky na unikátní výstupy
    - Definovat požadavky na obsah výstupů
    - Definovat četnost poskytovaných výstupů
    - Definovat vzhled
    - Definovat vlastnictví výstupu

Jak definovat požadavky na řešení

- Požadavky na user management
  - Definovat potřeby na základě jednotlivých rolí
    - Oddělení přístupů na základě role
    - Oddělení přístupu na základě geografické příslušnosti
    - Počty uživatelů
  - Definovat preferovaný typ klienta
    - Tlustý (vlastní aplikace na každé klientské stanici)
    - Tenký (webový)
  - Definovat další potřeby
    - Zabezpečení samotného rozhraní
    - Podpora LDAP/AD

Jak vybrat to správné řešení

- Splnění mandatorních požadavků
  - Množství logovaných událostí
    - Dokáže přijmout požadovaný počet událostí
    - Dokáže analyzovat požadovaný počet událostí
  - Podpora zásadního množství připojovaných zařízení
    - Čím více zařízení podporuje tím snazší a levnější je implementace
    - Aktualizace definic jednotlivých událostí
  - Podpora vyhodnocení definovaných bezpečnostních incidentů
  - Splnění požadavků na výstupy
  - Splnění nároků na user management
  - Možnost přidání vlastních zařízení

Jak vybrat to správné řešení

- Náročnost implementace
  - Počty jednotlivých HW a SW
    - Appliance
    - SW
    - HW + SW
  - Náročnost připojení jednotlivých zařízení
    - Nároky na připojení vlastních zdrojů událostí
  - Náročnost konfigurace vlastních zařízení
    - Nároky na konfiguraci samotného řešení
    - Nároky na patch management

Jak vybrat to správné řešení

- Náročnost konfigurace
  - Náročnost prvotní konfigurace
  - Náročnost konfigurace nově definovaných incidentů
  - Náročnost konfigurace výstupů
  - Náročnost na úpravy definovaných incidentů

Jak vybrat to správné řešení

- Cena za řešení a podporu
  - Cena za hw a sw komponenty
    - Cena definovaná dodávkou a možnostmi dodavatele
  - Cena za implementaci
    - Cena definovaná dodávkou a možnostmi dodavatele
  - Cena za podporu
    - Cena definovaná dodávkou a možnostmi dodavatele
    - Cena za případné úpravy

SECURITY 2011

19. ročník konference o bezpečnost v ICT

Děkujeme za pozornost.

Jan Svoboda

AEC

Jan.svoboda2@aec.cz