Implementace bezpečnosti a monitoringu IT infrastruktury

GERKIN s.r.o.

Jan Paleček

Extreme FORUM 2015

G E R K I N

Výchozí stav

- Nezkonsolidovaná infrastruktura různého stáří a od několika výrobců
- Nedostatek zkušeností a nedostatek zdrojů pro vytvoření vstupů
- Neexistující katalog služeb, koncepce a analýza rizik
- Neexistující sledování chování uživatele na síti
- Neexistující kontrola přístupů k síti
- Monitoring a management na opensource
  - Výstupy z monitoringu nejsou konsolidované

Požadavky na systematizace IT

- ISO 27000 vs. Zákon o kybernetické bezpečnosti
- Kontrola přístupů do LAN a vytvoření uživatelské databáze
- Autentizace uživatelů do LAN
- Kontrola uživatelů a jejich činnosti na LAN
- Kontrola systémových požadavků na aplikace
- Kontrola vytížení sítě aplikacemi => kontrola dostatečnosti systémových prostředků

Postup implementace monitoringu

- Instalace Purview
  - Po cca měsíci začínáme pracovat s ostrými daty
    - Vytížení HW na úrovni uživatelů a aplikací
    - Nekorektní chování uživatelů
    - Kontrola přístupu do sítě na úrovni OS
  - Předání podkladů zákazníkovi pro vytvoření katalogu služeb a definici bezpečnostních rizik
- Připojení všech spravovatelných zařízení do NetSightu
  - Definice rizik, kontrola zapojení a přiřazení stupně důležitosti

Postup implementace bezpečnosti

- Nasazení VLAN (kontrola nepoužívaných a jejich smazání, definice nových a implementace routovacích pravidel mezi VLAN)
- Implementace NAC přístupů do LAN a WiFi
- Nasazení SIEM na LAN a WiFi
- Nasazení a definování bezpečnostních skupin pro NAC a SIEM
- Pravidelná kontrola výstupů z Purview a implementace nových skupin a jejich pravidel

Výsledek a výhody

- Celá LAN pod jednotným managementem s výstupem na helpdesk
  - Bez ohledu na výrobce některých technologií
  - Lze zapojit téměř vše, co má IPv4 či IPv6
- Kontrola, monitoring a záznam o všech uživatelích přistupujících do LAN
- Kontrola, monitoring a záznam o vytíženosti jednotlivého HW pro aplikace

Děkuji za pozornost!

Jan Paleček

GERKIN s.r.o.

Jan.Palecek@Gerkin.cz