Kompleksowa konfiguracja systemu bezpieczeństwa ochrony sieci wraz z analizą i logowaniem zdarzeń, z wykorzystaniem urządzeń firmy FORTINET

Poznane produkty:

- FortiGate.
- FortiAnalyzer VM
- FortiCloud.

Cel szkolenia:

- Konfiguracja wielu łącz internetowych, backup i zarządzaniem pasmem.
- Opanowanie integracji urządzeń FortiGate z kontrolerem domeny oraz wykorzystanie tego połączenia do konfiguracji polityk bezpieczeństwa oraz zdalnego dostępu do zasobów sieci.
- Zaawansowana konfiguracja tuneli VPN pomiędzy urządzeniami oraz bezpieczny dostęp do zasobów sieci wewnętrznej.
- Gromadzenie logów oraz ich analiza i archiwizacja.

Forma zajęć:

- Praktyczne warsztaty z dostępem do samodzielnej konfiguracji urządzeń firmy Fortinet.

Prowadzący:

- Inżynier posiadający certyfikaty Network Security Expert oraz wieloletnie doświadczenie w zakresie wdrażania i wsparcia rozwiązań Fortinet.

Certyfikacja:

- Każdy uczestnik po pozytywnym zaliczeniu egzaminu na koniec szkolenia otrzymuje certyfikat.

Termin:

- 08-10 czerwiec 2022r.

Koszt szkolenia:

- 3500 PLN netto od osoby.

Czas trwania:

- 3 dni.

Miejsce:

- „Pensjonat Pod Tatrami”
  ul. Na Brzegu 21, 34-424 Szaflary.

Agenda:

1. Wstępne informacje o platformach Fortinet.
2. Debugowanie komunikacji z siecią FortiGuard.
3. Akceleracja sprzętowa w platformach Fortigate.
4. Definiowanie polityk bezpieczeństwa na urządzeniach Fortigate:
    a. Logowanie:
        - FortiAnalyzer,
        - Dysk,
        - Dodatkowe platformy logowania i raportowania,
        - Konfiguracja logowanych informacji: typy logów, poziomy logowania,
        - Logowanie do Syslog.
    b. FortiAnalyzer - omówienie platformy.
5. Analiza aktywności w sieci – FortiView.
6. Obsługa kilku łączy:
    a. Konfiguracja w oparciu o routing (priorytety, dystans, policy routing),
    b. Funkcja WAN Loadballancing:
        - Konfiguracja SD-WAN,
7. Uwierzytelnianie dwu-składnikowe – FortiToken:
    a. Przykład konfiguracji w oparciu o token mobilny.
8. Kontrola AV + Sandboxing.
9. Analiza ruchu szyfrowanego SSL:
    a. Omówienie trybów inspekcji.
10. Ochrona przed atakami IPS/IDS.

11. Konfiguracja profilu ochrony przed atakami i test działania.
12. Konfiguracja Webfiltering'u:
    a. Filtrowanie w oparciu o kategorie,
    b. White/Black listy stron.
12. DLP – ochrona przed wyciekiem informacji poufnej.
13. Ochrona poczty - Konfiguracja domeny chronionej.
14. Obsługa SMTP przez FortiMail.
15. FortiMail jako MTA dla poczty przychodzącej i wychodzącej:
    a. Weryfikacja adresów recipiet.
16. Konfiguracja i omówienie reguł Access Control:
    a. Niezbędne polityki do poprawnej obsługi ruchu.
    b. Ochrona przed open relay.
17. Omówienie zasad działania Polityk.
18. Profile antywirusowe.
19. Omówienie oraz konfiguracja Integracji z Sandbox.
20. Profile kontroli treści.
21. DLP.
22. Kwarantanna:
    a. Systemowa,
    b. Użytkownika.
23. Archiwizacja poczty w oparciu o polityki:
    a. Lokalna,
    b. Na zewnętrznych zasobach,
    c. Dostęp do archiwum poczty.
24. Szyfrowanie poczty w oparciu o polityki (IBE).