Kompleksowa konfiguracja systemu bezpieczeństwa ochrony sieci, ochrony poczty elektronicznej wraz z analizą logowaniem zdarzeń z wykorzystaniem rozwiązań marki FORTINET

Omawiane produkty:

- FORTINET **FortiGate**

- FORTINET **FortiAnalyzer**

- FORTINET **FortiMail**

Cel szkolenia:

- Zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji urządzeniami FortiGate. Poznanie najczęściej spotykanych zagrożeń oraz podstaw tworzenia i zarządzania polityką bezpieczeństwa na styku sieci lokalnej z Internetem.

- Zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji urządzeniem FortiAnalyzer. Poznanie funkcjonalności urządzenia, konfiguracji do współpracy z urządzeniami FortiGate oraz możliwości monitorowania i raportowania.

- Zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji urządzeniami FortiMail. Poznanie najczęściej spotykanych zagrożeń związanych z pocztą elektroniczną oraz sposobów ich zwalczania przy użyciu urządzeń FortiMail.

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 otrzymuje certyfikat.

Termin:

- 19 – 21 czerwiec 2024r.

Koszt szkolenia:

- 4500 PLN netto od osoby.

Czas trwania:

- 3 dni.

Miejsce:

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

Agenda:

Dzień 1.

1. Otwarcie szkolenia, lunch.
2. Kierunki rozwoju oraz możliwości sprzedażowe.

   – prezentacja właściciela firmy MS-IT Systemy Informatyczne.
3. Nowości w ofercie produktowej FORTINET.

   – prezentacja certyfikowanego Inżyniera Network Security Expert.
4. Uroczysta kolacja.

Dzień 2. – FortiGate

1. Wprowadzenie i wstępna informacje o platformach FortiGate
2. Definiowanie polityk zapory sieciowej,
   a) Zasady działania
   b) Tryby pracy
3. Translacja adresów sieciowych
   a) SNAT
   b) DNAT
4. Uwierzytelnianie użytkowników
   a) LDAP
   b) FSSO
   c) Uwierzytelnianie dwuskładnikowe - FortiToken
5. Logowanie i monitoring
   a) Typy logów
   b) Poziomy logowania
   c) Dysk
   d) FortiAnalyzer

6. Filtr stron www WebFilter
7. Kontrola aplikacji
8. Kontrola antywirusowa
    a) Ochrona przed nieznanymi zagrożeniami z wykorzystanie sandbox
9. System ochrony przed włamaniami
    a) IPS
    b) IDS
10. Koncepcja Security Fabric
11. Routing
    a) Routing statyczny
    b) Policy Routing
12. Zdalne połączenia SSL VPN
    a) Tryb tunelowy
    b) Tryb webowy
13. IPsec VPN
    a) Site to site
    b) Client to site
14. Diagnostyka
    a) Sniffer
    b) Debuf flow

Dzień 3. – FortiMail

1. Wprowadzenie i wstępna konfiguracja FortiMail w trybie Gateway
2. Konfiguracja domeny chronionej
3. Obsługa ruchu SMTP przez FortiMail
4. Omówienie zasad działania polityk
    a) Access Controll
    b) IP Policy
    c) Recipient Policy
5. Analiza logów
6. Omówienie i konfiguracja profilu sesji
7. Profile antyspamowe
8. Profile antywirusowe
    a) Ochrona przed nieznanymi zagrożeniami z wykorzystanie sandbox
9. Konfiguracja profili kontroli treści
10. DLP
11. White/Black listy
12. Kwarantanna
    a) Systemowa
    b) Użytkownika
13. Integracja z LDAP
14. Archiwizacja poczty w oparciu o polityki
15. Szyfrowanie poczty w oparciu o polityki (IBE)
16. Raportowanie
17. Przechowywanie poczty na zewnętrznych zasobach
18. Kopie zapasowe