



Opis przedmiotu zamówienia

Szkolenie specjalistyczne dla kadry zarządzającej i informatyków w zakresie planowanych do zastosowania środków bezpieczeństwa w ramach projektu grantowego

Cel szkolenia: podniesienie kompetencji z zakresu cyberbezpieczeństwa i zapoznanie się z zasadami i narzędziami z zakresu bezpieczeństwa cyfrowego, które są wdrażane w jednostce.

Grupa docelowa: Kadra zarządzająca i Informatycy Urzędu Gminy Zbuczyn oraz jednostek organizacyjnych

Tryb szkolenia: stacjonarnie

Liczba uczestników: 8

Sale szkoleniowe: szkolenia realizowane w Sali zapewnionej przez Zamawiającego

Liczba godzin szkoleniowych: minimum 4 godz. (1 godz. szkoleniowa = 45 minut)

Catering podczas szkoleń: po stronie Zamawiającego

Materiały szkoleniowe: po stronie Wykonawcy

Dokumentacja szkolenia:

Ponadto Wykonawca zobowiązany jest do:

- zapewnienia każdemu uczestnikowi imiennego certyfikatu/zaświadczenia potwierdzającego ukończenie szkolenia,
- prowadzenia listy obecności (podpisy/logi),
- oznaczenia wszelkich materiałów, prezentacji i innych dokumentów opracowanych na potrzeby szkolenia zgodnie z wymaganiami regulaminu konkursu „Cyberbezpieczny Samorząd”, umowy o powierzenie grantu oraz wniosku o dofinansowanie

Program szkolenia powinien obejmować co najmniej następujące zagadnienia:

Moduł 1: Wprowadzenie i Kontekst Projektu Grantowego

Cel: Zrozumienie "dlaczego" wdrażamy te narzędzia.

Zagadnienia:

- Przedstawienie celów projektu grantowego i jego znaczenia dla organizacji.
- Aktualny krajobraz zagrożeń cybernetycznych i ryzyka specyficzne dla organizacji.
- Ogólna strategia cyberbezpieczeństwa organizacji i miejsce nowych narzędzi w tej strategii.
- Podstawowe wymogi prawne i regulacyjne (np. RODO) a nowe narzędzia.
- Rola kadry zarządzającej i IT w sukcesie wdrożenia i utrzymania bezpieczeństwa.

Moduł 2: Monitoring i Zarządzanie Infrastrukturą

Cel: Zrozumienie możliwości monitorowania sieci, zasobów i użytkowników.

Zagadnienia:

- Korzyści z centralnego monitoringu (widoczność, kontrola kosztów IT, bezpieczeństwo danych).
- Przegląd kluczowych raportów i dashboardów (wykorzystanie zasobów, aktywność użytkowników, alerty bezpieczeństwa).
- Rola nVision (lub równoważny) we wspieraniu zgodności (np. inwentaryzacja oprogramowania).

Moduł 3: Centralne Zarządzanie Logami i Zdarzeniami



Cel: Zrozumienie znaczenia logów dla bezpieczeństwa i zgodności oraz możliwości ich centralnej analizy.

Zagadnienia:

- Dlaczego zbieranie i analiza logów jest krytyczna (wykrywanie incydentów, audyty, zgodność z RODO).
- Koncepcja SIEM (Security Information and Event Management) – co nam to daje?
- Przykładowe raporty dla zarządu (trendy bezpieczeństwa, status zgodności).

Moduł 4: Ochrona Stacji Końcowych i Serwerów

Cel: Zrozumienie warstwowej ochrony punktów końcowych.

Zagadnienia:

- Rodzaje zagrożeń dla stacji roboczych i serwerów (malware, ransomware, phishing).
- Kluczowe funkcje ochrony (antywirus, firewall)
- Znaczenie centralnego zarządzania i spójnych polityk bezpieczeństwa.

Moduł 5: Backup i Odzyskiwanie Danych

Cel: Zrozumienie strategii ochrony danych przed utratą i zapewnienia ciągłości działania.

Zagadnienia:

- Znaczenie backupu dla ciągłości biznesowej (awarie, ataki ransomware, błędy ludzkie).
- Podstawowe pojęcia: RPO (Recovery Point Objective) i RTO (Recovery Time Objective).
- Koszty przestoju a inwestycja w backup.
- Wymogi RODO dotyczące kopii zapasowych.

Moduł 6: Bezpieczeństwo Sieci

Cel: Zrozumienie roli zapory sieciowej nowej generacji w ochronie perymetru sieci.

Zagadnienia:

- Koncepcja ochrony brzegowej (firewall, VPN, filtrowanie treści).
- Jak FortiGate (lub równoważny) chroni przed zagrożeniami z Internetu?
- Widoczność ruchu sieciowego i kontrola dostępu.

Moduł 7: Ochrona Przed Wyciekami

Cel: Zrozumienie ryzyka wycieku danych i sposobów jego minimalizacji.

Zagadnienia:

- Ryzyko związane z utratą danych wrażliwych (dane osobowe, tajemnice handlowe).
- Wymagania RODO dotyczące ochrony danych.
- Koncepcja DLP (Data Loss Prevention) – jak działa i co chroni?
- Monitorowanie przepływu danych i identyfikacja ryzykownych zachowań (bez naruszania prywatności).
- Przegląd raportów dla zarządu (incydenty DLP, trendy).

Moduł 8: Integracja i Synergia Narzędzi

Cel: Pokazanie, jak narzędzia współpracują, tworząc kompleksowy system ochrony.

Zagadnienia:

- Podkreślenie korzyści z podejścia warstwowego i zintegrowanego.