Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

E- standardy bezpiecznego kodowania

Cele szkolenia

Celem szkolenia jest wyposażenie uczestników w wiedzę i praktyczne umiejętności niezbędne do pisania kodu odpornego na ataki, projektowania bezpiecznego oraz zgodne z prawem oprogramowania, a także wdrożenia wymogów prawnych Unii Europejskiej w codziennej pracy deweloperskiej.

Umiejętności

Dzięki szkoleniu uczestnik będzie:

- Rozróżniać rodzaje danych (osobowe, nieosobowe, quasi-identyfikatory, atrybuty wrażliwe) oraz procesy ich przetwarzania zgodnie z RODO i Data Act.
- Wdrażać zasady Privacy by Design, Privacy by Default oraz Privacy by Security na każdym etapie architektury i cyklu życia oprogramowania (SSDLC).
- Skutecznie stosować techniki ochrony prywatności danych, takie jak anonimizacja (modele K-anonimowości, L-różnorodności, T-bliskości) oraz pseudonimizacja (tokenizacja, hashowanie, szyfrowanie).
- Identyfikować i minimalizować ryzyko reidentyfikacji danych przy użyciu analizy ryzyka (DPIA).
- Przewidywać i wykrywać luki bezpieczeństwa za pomocą modelowania zagrożeń (metodyka STRIDE, OWASP Threat Dragon) oraz narzędzi SAST i SCA.
- Projektować bezpieczne mechanizmy uwierzytelniania, autoryzacji (RBAC, ABAC, ReBAC) oraz bezpiecznego zarządzania sesją (atrybuty cookies, mechanizmy timeoutów).
- Świadomie i odpowiedzialnie korzystać z generatywnej sztucznej inteligencji (Gen AI) w procesie programowania, minimalizując ryzyko halucynacji i wycieku danych poufnych.

Profil uczestników

Szkolenie przeznaczone jest dla programistów, inżynierów oprogramowania, architektów systemów IT, liderów zespołów deweloperskich, testerów oraz specjalistów ds. cyberbezpieczeństwa i compliance, którzy chcą podnieść swoje kwalifikacje w zakresie tworzenia bezpiecznego kodu i ochrony danych osobowych.

Przygotowanie uczestników

Od uczestników wymagana jest podstawowa znajomość dowolnego języka programowania oraz fundamentalnych pojęć z zakresu architektury aplikacji webowych lub mobilnych. Wcześniejsza znajomość przepisów prawnych z zakresu ochrony danych nie jest wymagana.

Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

Szczegółowy program szkolenia

1. Wprowadzenie i cel szkolenia

- Organizacja szkolenia
- Poruszanie się po kursie
- Przewodnik po kursie
- Filozofia bezpieczeństwa

2. Bezpieczeństwo informacji w procesie kodowania

- Prawo UE a system krajowy
- Akty prawne
- Dane w IT
- Standardy ochrony prywatności
- Zarządzanie ryzykiem biznesowym

3. Podstawy prawne przetwarzania danych osobowych

- Podstawy prawne wg RODO
- Zgoda użytkownika
- Wdrożenie techniczne i dokumentacyjne

4. Anonimizacja danych

- Definicja
- Status prawny
- Zarządzanie ryzykiem
- Modele zaawansowanej anonimizacji
- Techniki uzupełniające
- Cykl procesu

5. Pseudonimizacja danych

- Definicja
- Porównanie
- Techniki pseudonimizacji:

- Architektura bezpieczeństwa
- Wyzwania wdrożeniowe

6. Reidentyfikacja danych

- Zjawisko reidentyfikacji
- Profil atakującego
- Wektory ataku
- Trzy filary ochrony

7. Bezpieczny cykl życia oprogramowania (SSDLC)

- Porównanie modeli
- Praktyki bezpieczeństwa na etapach projektu

8. Modelowanie zagrożeń i standard STRIDE

- Podejście ustrukturyzowane
- Analiza kategorii zagrożeń STRIDE
- Narzędzia

9. Zarządzanie zależnościami i bezpieczne kodowanie

- Zagrożenia zewnętrze
- Wektory infekcji
- Narzędzia klasy SCA (Software Composition Analysis)
- Zarządzanie komponentami
- Obsługa podatności
- Code Review

10. Uwierzytelnienie, autoryzacja i modele kontroli dostępu

- Ochrona kont
- Polityka haseł
- Mechanizmy obronne
- Procedura resetowania haseł
- Modele autoryzacji
- Ochrona zasobów

11. Bezpieczne zarządzanie sesją, logowanie i obsługa błędów

- Cykl życia sesji
- Atrybuty bezpieczeństwa cookies
- Mechanizmy wygasania sesji
- Zarządzanie stanem sesji
- Logowanie zdarzeń (Logging
- Obsługa błędów
- Ochrona sieciowa

12. Kryptografia i zarządzanie sekretami

- Fundamenty kryptografii
- Przechowywanie haseł
- Standardy algorytmiczne
- Ochrona danych w locie i w spoczynku
- Zarządzanie sekretami:

13. Bezpieczeństwo specyficzne dla platform i REST API

- Projektowanie REST API
- Autoryzacja tokenowa
- Kontrola ruchu
- Wersjonowanie API
- Specyfika platform mobilnych

Metoda realizacji szkolenia

Kurs realizowany jest w nowoczesnej formule w pełni zdalnego, samodzielnego kształcenia(self-learning) osadzonego na platformie LMS Comarch. Materiał został podzielony na moduły tematyczne zawierające bogate treści teoretyczne, prezentacje multimedialne, interaktywne schematy warstwowe i przepływów danych oraz studia przypadków. Każdy moduł kończy się praktycznym quizem utrwalającym, a całe szkolenie zwieńczone jest oficjalnym, przekrojowym testem wiedzy.

Wymagania formalne zaliczenia kursu: Szkolenie kończy się oficjalnym testem wiedzy składającym się z 18 pytań testowych jednokrotnego lub wielokrotnego wyboru oraz zadań typu dopasowanie pojęć. Próg zaliczenia uprawniający do uzyskania certyfikatu wynosi 80%