



Niebezpiecznik.pl

Piotr Konieczny

★★★★★ 4,7 / 5

30 ocen

Szkolenie z Cyberbezpieczeństwa: Bezpieczeństwo aplikacji mobilnych (atak i ochrona)

Numer usługi 2026/08/11/148153/3740814

📍 Kraków

🏢 Usługa szkoleniowa

📅 stacjonarna

👥 Zajęcia grupowe

🕒 14:00 h

📅 30.12.2026 do 31.12.2026

7 242,24 PLN brutto

5 888,00 PLN netto

517,30 PLN brutto/h

420,57 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie kierujemy przede wszystkim do osób, których praca ociera się o aplikacje mobilne, a więc: • programistów i testerów, • administratorów oraz architektów i projektantów rozwiązań mobilnych • audytorów i pentesterów, ...ale tak naprawdę, z otwartymi rękami powitamy każdą osobę która chce podnosić swoje kwalifikacje i wiedzę w temacie bezpieczeństwa aplikacji mobilnych – dla nas wszyscy jesteście żądnymi wiedzy ludźmi, a nie stanowiskami ;-)
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	22-12-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Głównym celem szkolenia jest dostarczenie oraz poprawienie kompetencji uczestnika z zakresu Bezpieczeństwa aplikacji mobilnych. Po zakończonym szkoleniu uczestnik podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Dowiesz się w jaki sposób można zabezpieczyć aplikacje mobilne przed atakami, poznasz techniki ataków na aplikacje mobilne wykorzystywane przez współczesnych włamywaczy, nauczysz się korzystać z kilkudziesięciu narzędzi do testowania bezpieczeństwa aplikacji, wprowadzisz mechanizmy utrudniające inżynierię wsteczną aplikacji mobilnej, wykonasz dziesiątki praktycznych ćwiczeń na realnym sprzęcie.	Laboratoria przygotowane na symulowanym środowisku kształcenia.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

<https://niebezpiecznik.pl/szkolenia/bezpieczenstwo-aplikacji-mobilnych/?zai>

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

1. Architektury mobilnych systemów operacyjnych

- iOS
- Android

2. Bezpieczeństwo z perspektywy użytkownika urządzenia:

- domyślnie dostępne sposoby zabezpieczeń urządzeń w danych systemach
- wpływ domyślnych zabezpieczeń urządzeń na bezpieczeństwo aplikacji
- data wiping

3. Mechanizmy bezpieczeństwa dostarczane developerom przez producentów systemów. Między innymi:

- system uprawnień (Android)
- Data Protection (iOS)
- Keychain (iOS)

4. Przełamywanie zabezpieczeń systemów:

- eskalacja uprawnień w systemach mobilnych (jailbreak)
- wpływ eskalacji uprawnień na bezpieczeństwo aplikacji
- dostęp do danych użytkowników (m.in. SMS, e-mail, dane GPS)
- analiza systemu plików (ich struktur i typów)
- przełamywanie szyfrowania danych

5. Bezpieczeństwo danych:

- zagrożenia związane z wykradaniem danych na przykładzie prawdziwych zdarzeń
- sposoby bezpiecznego przechowywania kluczowych danych (login, hasło, klucze, dane osobowe)
- implementowanie szyfrowania w aplikacjach mobilnych
- zabezpieczanie aplikacji hasłem dostępowym
- bezpieczna komunikacja pomiędzy aplikacjami (wymiana danych) oraz komponentami (Android: Activity, Service, Broadcast receiver, Content Resolver)
- szyfrowanie baz danych

6. Bezpieczeństwo komunikacji:

- zagrożenia płynące z "transportu" danych
- poprawna, bezpieczna implementacja aplikacji klient-serwer
- mechanizmy szyfrowania (SSL/TLS)
- wykorzystanie PKI (Public Key Infrastructure)

7. Bezpieczeństwo aplikacji:

- analiza sposobów dystrybucji aplikacji i ryzyka z nią związane
- analiza form binarnych aplikacji i ich dystrybucji (m.in. odex, Mach-O, ipa, apk)
- Reverse Engineering aplikacji (m.in. Cycrypt, baksmali, apktool)
- utrudnianie analizy kodu i modyfikacji działania aplikacji (m.in. blokowanie debuggerów, obfuskacja kodu, ASLR)

- wykrywanie środowisk z podwyższonymi uprawnieniami (jailbreak)
 - narzędzia wspomagające analizę bezpieczeństwa aplikacji
8. Istotne mechanizmy specyficzne dla platform i ataki z nimi związane. Między innymi:
- multitasking (app state/GUI caching)
 - wprowadzanie danych (input caching)
 - zanużanie aplikacji webowych (CSRF, framing, clickjacking)
 - identyfikacja urządzeń i użytkowników (UDID)
 - push notifications
 - tapjacking
 - zarządzanie logami
9. Ciekawe przypadki przełamывania zabezpieczeń – case studies.

Harmonogram

Liczba pozycji harmonogramu: 12

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Architektury mobilnych systemów operacyjnych	Zajęcia	Mateusz Biliński	30-12-2026	10:00	12:00	02:00
2 z 12 Bezpieczeństwo z perspektywy użytkownika urządzenia	Zajęcia	Mateusz Biliński	30-12-2026	12:00	13:00	01:00
3 z 12 -	Przerwa	-	30-12-2026	13:00	14:00	01:00
4 z 12 Mechanizmy bezpieczeństwa dostarczane developerom przez producentów systemów.	Zajęcia	Mateusz Biliński	30-12-2026	14:00	16:00	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 12 Przełamywani e zabezpieczeń systemów	Zajęcia	Mateusz Biliński	30-12-2026	16:00	17:00	01:00
6 z 12 Bezpieczeńst wo danych	Zajęcia	Mateusz Biliński	31-12-2026	10:00	11:00	01:00
7 z 12 Bezpieczeńst wo komunikacji	Zajęcia	Mateusz Biliński	31-12-2026	11:00	12:00	01:00
8 z 12 Bezpieczeńst wo aplikacji	Zajęcia	Mateusz Biliński	31-12-2026	12:00	13:00	01:00
9 z 12 -	Przerwa	-	31-12-2026	13:00	14:00	01:00
10 z 12 Istotne mechanizmy specyficzne dla platform i ataki z nimi związane.	Zajęcia	Mateusz Biliński	31-12-2026	14:00	15:00	01:00
11 z 12 Ciekawe przypadki przełamywani a zabezpieczeń – case studies.	Zajęcia	Mateusz Biliński	31-12-2026	15:00	16:00	01:00
12 z 12 -	Walidacja	-	31-12-2026	16:00	17:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	14:00
w tym suma godzin zajęć	11:00
w tym suma godzin walidacji	01:00
w tym suma przerw	02:00

Rodzaj godzin	Liczba godzin
Suma godzin dydaktycznych bez przerw	16:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania ze zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

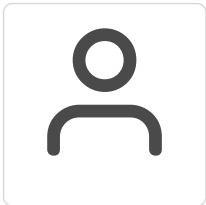
Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 242,24 PLN
Koszt przypadający na 1 uczestnika netto	5 888,00 PLN
Koszt osobogodziny brutto	517,30 PLN
Koszt osobogodziny netto	420,57 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	14:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Mateusz Biliński

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

1. Materiały szkoleniowe (zapis prezentacji).

Warunki uczestnictwa

Każdy uczestnik naszych szkoleń **musi** podpisać deklarację, że poznane ataki i narzędzia będzie wykorzystywał wyłącznie w celu testowania bezpieczeństwa swoich własnych aplikacji.

Szkolenie realizowane w formule Bring Your Own Device.

Wymagane: komputer z system operacyjnym na architekturę 64bit i najnowszą wersją programu Virtualbox (min. 4 GB RAM-u – zalecane 6GB) oraz co min. 20GB wolnego miejsca na HDD. Do pełnego, aktywnego uczestnictwa w kilku labach wymagane jest urządzenie z systemem iOS w wersji 8.0 lub wyższej, na którym można przeprowadzić jailbreak, oraz komputer z systemem Mac OS X (wymagane dla osób skupionych na platformie iOS - system zawiera bowiem narzędzia przygotowane do pracy na architekturze ARM i plikach w formacie Mach-O).

Brak spełnienia powyższych wymagań nie uniemożliwia przejścia przez laboratoria, ale sprawi, że uczestnik będzie musiał zadowolić się demonstracją pokazaną przez trenera (jeśli iOS nie leży w głównych zainteresowaniach uczestnika).

Informacje dodatkowe

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

<https://niebezpiecznik.pl/szkolenia/bezpieczenstwo-aplikacji-mobilnych/?zai>

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

Szkolenie trwa 14 godzin zegarowych.

Godziny, o której będą przerwy są ustalane przez trenera i uczestników w trakcie szkolenia:

1 przerwa obiadowa 30-minutowa

2 przerwy kawowe 15-minutowe

Adres

ul. Armii Krajowej 11

30-150 Kraków

woj. małopolskie

Szczegóły miejsca realizacji usługi wysyłane są do Uczestników szkolenia na tydzień przed danym terminem.

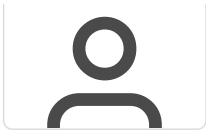
Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt



Magda Kowalska



E-mail szkolenia@niebezpiecznik.pl

Telefon (+48) 124 420 244