Możliwość dofinansowania

# Szkolenie z Cyberbezpieczeństwa: Bezpieczeństwo aplikacji mobilnych: Android

**Numer usługi** 2026/02/04/148153/3306997

4 290,24 PLN brutto
3 488,00 PLN netto
612,89 PLN brutto/h
498,29 PLN netto/h
261,33 PLN cena rynkowa

Niebezpiecznik.pl
Piotr Konieczny

4,7 / 5

30 ocen

Kraków
Usługa szkoleniowa
stacjonarna
07:00 h
17.07.2026 do 17.07.2026

# 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:<br>• programistów i testerów,<br>• administratorów oraz architektów i projektantów rozwiązań mobilnych<br>• audytorów i pentesterów,<br>...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** | 09-07-2026 |
| **Forma prowadzenia usługi** | stacjonarna |
| **Liczba godzin usługi** | 7 |
| **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 w systemie Android. 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,<br>poznasz techniki ataków na aplikacje mobilne wykorzystywane przez współczesnych włamywaczy,<br>nauczysz się korzystać z kilkudziesięciu narzędzi do testowania bezpieczeństwa aplikacji,<br>wprowadzisz mechanizmy utrudniające inżynierię wsteczną aplikacji mobilnej,<br>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 zawiera opis efektów uczenia się?**

TAK

**Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?**

TAK

**Pytanie 3. Czy dokument potwierdza 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-android/?zai

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

**1. Wstęp do systemów mobilnych, aplikacji oraz wprowadzające przykłady błędów.**

**2. Architektura systemu Android z perspektywy systemu i działania aplikacji.**

**3. Mechanizmy bezpieczeństwa dostarczane twórcom aplikacji androidowych, m.in:**

• system uprawnień

• KeyStore

• deklaratywna konfiguracja sieci

• key attestation

**4. Przełamywanie zabezpieczeń systemów:**

• eskalacja uprawnień w systemach mobilnych (rootowanie)

• wpływ eskalacji uprawnień na bezpieczeństwo aplikacji

• dostęp do danych użytkowników (m.in. SMS, e-mail, dane GPS)

• wpływ stanu systemu i urządzenia na bezpieczeństwo aplikacji

**5. Bezpieczeństwo danych:**

• zagrożenia związane z wykradaniem danych na przykładzie prawdziwych zdarzeń

• sposoby bezpiecznego przechowywanie kluczowych danych (login, hasło, klucze,

dane osobowe)

• wykorzystywanie szyfrowania w aplikacjach mobilnych (standardy, dobre praktyki, implementacje)

• zabezpieczanie dostępu do aplikacji (hasła, biometryka, 2FA)

• bezpieczna komunikacja pomiędzy aplikacjami (wymiana danych) oraz

komponentami (Activity, Service, Broadcast Receiver, Content Provider)

• szyfrowanie (baz) danych

**6. Bezpieczeństwo komunikacji:**

• zagrożenia płynące z “transportu” danych

• poprawna, bezpieczna implementacja aplikacji klienckich

• mechanizmy szyfrowania (SSL/TLS)

• wykorzystanie PKI (Public Key Infrastructure)

• poziomy zabezpieczania poufności i integralności komunikacji

• pinning i jego warianty

• polecane biblioteki i implementacje

**7. Bezpieczeństwo aplikacji:**

• analiza sposobów dystrybucji aplikacji i ryzyka z nią związane

• analiza form binarnych aplikacji i ich dystrybucji

• Reverse Engineering aplikacji (m.in. baksmali, apktool, jadx)

• utrudnianie analizy kodu i modyfikacji działania aplikacji (m.in. blokowanie debuggerów, obfuskacja kodu, ASLR, zanurzanie interpreterów, wielojęzykowość)

• wykrywanie środowisk z podwyższonymi uprawnieniami (zrootowane)

• narzędzia wspomagające analizę bezpieczeństwa aplikacji

**8. Istotne mechanizmy specyficzne dla platform i ataki z nimi związane, m.in.:**

• multitasking (app state/GUI caching)

• wprowadzanie danych (input caching)

• zarządzanie logami

• kopie zapasowe (danych) aplikacji

• uprawnienia i komunikacja między procesami

**9. Ciekawe przypadki przełamywania zabezpieczeń – case studies.**

# Harmonogram

Liczba pozycji harmonogramu: 9

| Przedmiot / temat | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 1 z 9 Wstęp do systemów mobilnych, aplikacji oraz wprowadzające przykłady błędów. | Mateusz Biliński | 17-07-2026 | 10:00 | 10:30 | 00:30 |
| 2 z 9 Architektura systemu Android z perspektywy systemu i działania aplikacji. | Mateusz Biliński | 17-07-2026 | 10:30 | 11:00 | 00:30 |
| 3 z 9 Mechanizmy bezpieczeństwa dostarczane twórcom aplikacji androidowych | Mateusz Biliński | 17-07-2026 | 11:00 | 12:00 | 01:00 |
| 4 z 9 Przełamywanie zabezpieczeń systemów | Mateusz Biliński | 17-07-2026 | 12:00 | 13:00 | 01:00 |

| Przedmiot / temat | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 5 z 9 Bezpieczeństwo danych | Mateusz Biliński | 17-07-2026 | 13:00 | 14:00 | 01:00 |
| 6 z 9 Bezpieczeństwo komunikacji | Mateusz Biliński | 17-07-2026 | 14:00 | 15:00 | 01:00 |
| 7 z 9 Bezpieczeństwo aplikacji | Mateusz Biliński | 17-07-2026 | 15:00 | 16:00 | 01:00 |
| 8 z 9 Istotne mechanizmy specyficzne dla platform i ataki z nimi związane | Mateusz Biliński | 17-07-2026 | 16:00 | 16:30 | 00:30 |
| 9 z 9 Ciekawe przypadki przełamywania zabezpieczeń – case studies. | Mateusz Biliński | 17-07-2026 | 16:30 | 17:00 | 00:30 |

# Cennik

## Cennik

| Rodzaj ceny | Cena |
|---|---|
| **Koszt przypadający na 1 uczestnika brutto** | 4 290,24 PLN |
| **Koszt przypadający na 1 uczestnika netto** | 3 488,00 PLN |
| **Koszt osobogodziny brutto** | 612,89 PLN |
| **Koszt osobogodziny netto** | 498,29 PLN |

# 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 jest realizowane w formule BYOD – Bring Your Own Device. Uczestnik szkolenia MUSI POSIADAĆ komputer z system operacyjnym Windows (rekomendowane), MacOS(rekomendowane) lub Linux (wymaga więcej doświadczenia); Co najmniej 4 GB RAM-u (zdecydowanie zalecane 6GB i więcej); Co najmniej 25 GB wolnego miejsca na HDD. BARDZO DOBRZE BY BYŁO, gdyby komputer posiadny przez uczestnika posiadał procesor na architekturę x86_x64 (Intel 64-bit). Umożliwi to zainstalowanie i wykorzystanie programu VirtualBox do szybkiego przygotowania środowiska laboratoryjnego (wszystkie narzędzia w jednym miejscu). UWAGA: możliwe jest wykorzystanie komputerów z architekturą arm64 (np. MacBooki z M1/M2), natomiast będzie to wymagało wykonania dodatkowych kroków w celu przygotowania środowiska.

## Informacje dodatkowe

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

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

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

Szkolenie trwa 7 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