Rozwiązania Webowe

Bezpieczeństwo

Dr inż. Arkadiusz Rzucidło, prof. PRz

Fundamenty bezpieczeństwa w aplikacjach. Dlaczego bezpieczeństwo jest kluczowe?

- dane jako wartość
- ataki są powszechne
- systemy są publicznie dostępne
- użytkownik jako słabe ogniwo
- konsekwencje naruszeń

Fundamenty bezpieczeństwa w aplikacjach. Dlaczego bezpieczeństwo jest kluczowe?

- Każda aplikacja webowa jest dostępna przez Internet - **czyli dla wszystkich**, nie tylko dla użytkowników.
- To oznacza: **ktoś zawsze próbuje ją zaatakować**
- Dane to dziś najcenniejszy zasób:
  - dane użytkowników
  - dane finansowe
  - dane firmowe
- Najczęstszy problem:
  - **nie technologia, tylko użytkownik** (kliknięcie w zły link)

Fundamenty bezpieczeństwa w aplikacjach. Dlaczego bezpieczeństwo jest kluczowe?

Dlaczego aplikacje webowe są szczególnie narażone na ataki?

A. Bo działają wolniej niż desktopowe
B. Bo korzystają z baz danych
C. Bo są dostępne publicznie przez Internet
D. Bo nie używają systemu operacyjnego

Trzy filary bezpieczeństwa (CIA)

- poufność (**C**onfidentiality) – chronione tylko dla właściwych osób
- integralność (**I**ntegrity) – właściwe i poprawne dane
- dostępność (**A**vailability) – dostęp do uprawnionych
- ochrona danych
- ciągłość działania

Trzy filary bezpieczeństwa (CIA)

- Bezpieczeństwo to nie „czy działa”, tylko:
  - czy dane są bezpieczne (poufność)
  - czy nie są zmienione (integralność)
  - czy system działa (dostępność)

Przykład:

- bank działa → dostępność
- saldo poprawne → integralność
- dane nie wyciekają → poufność

Trzy filary bezpieczeństwa (CIA)

Który element CIA oznacza ochronę przed nieautoryzowanym dostępem do danych?

A. Integralność
B. Poufność
C. Dostępność
D. Skalowalność

Szyfrowanie (HTTPS)

- HTTP vs HTTPS
- szyfrowanie danych
- certyfikaty SSL/TLS
- bezpieczna transmisja
- ochrona przed podsłuchem

Szyfrowanie (HTTPS)

- HTTPS to absolutna podstawa.
- Bez niego:
  - dane lecą „otwartym tekstem”
- Z nim:
  - dane są zaszyfrowane

Przykład:

- logowanie bez HTTPS = hasło może zostać przechwycone

Szyfrowanie (HTTPS)

Co zapewnia HTTPS w aplikacji webowej?

A. Szybsze ładowanie strony, szczególnie w obciążonym środowisku
B. Lepszy, bardziej zawansowany wygląd strony
C. Przechowywanie danych w sposób bezpieczny
D. Szyfrowanie komunikacji między klientem a serwerem

Certyfikaty SSL/TLS

- potwierdzają tożsamość serwera
- wydawane przez CA
- przeglądarka weryfikuje
- zielona kłódka
- zapobieganie podszywaniu się

Certyfikaty SSL/TLS

- Certyfikat mówi:
  - „to naprawdę ten serwer, z którym chcesz się połączyć”
- Bez niego:
  - ktoś może podszyć się pod stronę banku
- To ochrona przed atakiem MITM (man-in-the-middle) – podsłuchiwanie (sniffing)

Certyfikaty SSL/TLS

Jaka jest główna rola certyfikatu SSL?

A. Potwierdzenie tożsamości serwera
B. Przyspieszenie Internetu podczas transmisji webowej
C. Zarządzanie aktualnością wpisów DNS
D. Przechowywanie danych w przeglądarce

Hasła i uwierzytelnianie

- silne hasła
- unikalność haseł
- przechowywanie (hashowanie)
- logowanie użytkownika
- ataki brute-force

Hasła i uwierzytelnianie

- Hasło to pierwsza linia obrony.
  - 12 znaków,
  - unikalność,
  - złożoność,
  - brak oczywistości
- Błędy:
  - „123456”
  - to samo hasło wszędzie
- W systemie:
  - hasła nie są przechowywane jako tekst
  - są hashowane (zabezpieczone)

Hasła i uwierzytelnianie

Dlaczego hasła są przechowywane w formie hasha?

A. Aby system mógł je szybciej znaleźć w bazie danych.
B. Aby uniemożliwić odczytanie ich w przypadku wycieku danych
C. Aby je łatwo odczytać przez systemu weryfikacji hasła w aplikacjach
D. Aby przyspieszyć logowanie, z hashowanymi hasłami dzieje się to automatycznie

Uwierzytelnianie dwuskładnikowe (2FA)

- coś co znasz (hasło)
- coś co masz (telefon)
- kod SMS / aplikacja
- zwiększenie bezpieczeństwa
- ochrona kont

Uwierzytelnianie dwuskładnikowe (2FA)

- Hasło to za mało.
- 2FA dodaje drugi element:
  - kod SMS
  - aplikacja (Google Authenticator)
  - tokeny
- Nawet jeśli ktoś pozna hasło:
  - nie zaloguje się bez drugiego składnika
- Klucze autoryzujące

Uwierzytelnianie dwuskładnikowe (2FA)

Dlaczego 2FA znacząco zwiększa bezpieczeństwo konta?

A. Zdecydowanie przyspiesza logowanie do systemu
B. Zastępuje hasło, mniej do pamiętania stąd łatwiej
C. Wymaga dodatkowego potwierdzenia poza hasłem
D. Ukrywa adres IP dzięki czemu intruzowi trudniej się włamać

Phishing

- podszywanie się pod zaufane strony
- fałszywe e-maile
- kradzież danych logowania
- manipulacja użytkownikiem
- najczęstszy typ ataku

Phishing

- Phishing nie atakuje systemu - tylko człowieka
- To rodzaj socjotechniki

Przykład:

- „Twoje konto zostało zablokowane – kliknij tutaj”
- Użytkownik:
  - wpisuje login i hasło
  - dane trafiają do atakującego

Phishing

Co jest głównym celem ataku phishingowego?

A. Uszkodzenie serwera i zablokowanie przed ponownym uruchomieniem
B. Spowolnienie Internetu – zapchanie sieci fałszywymi komunikatami
C. Zmiana adresu IP w celu zmiany zapisów w DNS
D. Pozyskanie danych użytkownika poprzez manipulację

Atak Man-in-the-Middle (MITM)

- przechwytywanie komunikacji
- podsłuch danych
- fałszywe sieci Wi-Fi
- brak szyfrowania = duże ryzyko
- ochrona: HTTPS

Atak Man-in-the-Middle (MITM)

- MITM = ktoś „w środku komunikacji”
  - użytkownik ↔ atakujący ↔ serwer

Przykład:

  - publiczne Wi-Fi
  - brak HTTPS
    - dane mogą być przechwycone

Atak Man-in-the-Middle (MITM)

Kiedy atak MITM jest najbardziej skuteczny?

A. Przy szybkim Internecie, trudno wyłapać wtedy niebezpieczne pakiety
B. Przy silnym haśle, to złudny atut, który wykorzystuje atakujący
C. Gdy komunikacja nie jest szyfrowana (brak HTTPS)
D. Przy użyciu DNS, atakujący wprowadza zmiany w zapisach DNS i myli systemy

SQL Injection (powiązanie z bazami)

- wstrzykiwanie zapytań SQL
- brak walidacji danych
- dostęp do bazy danych
- manipulacja danymi
- jeden z najgroźniejszych ataków

SQL Injection (powiązanie z bazami)

- To bezpośrednie połączenie z wcześniejszym wykładem.
  - użytkownik wpisuje dane
  - backend przekazuje je do SQL
- Jeśli brak zabezpieczeń:
  - atakujący może wykonać własne zapytanie
- Atak zwykle dotyczy niepoprawnie projektowanych systemów
- Ochrona to modyfikacja kodu web-aplikacji na bezpieczniejszy

SQL Injection (powiązanie z bazami)

Dlaczego SQL Injection jest tak groźny?

A. Pozwala na bezpośredni dostęp do bazy danych
B. Spowalnia sieć w wyniku czego system nie funkcjonuje poprawnie
C. Atakuje frontend i zmienia kod interfejsu użytkownika
D. Zmienia DNS przez co systemy są zdezorientowane

XSS (Cross-Site Scripting)

- wstrzykiwanie kodu JavaScript
- atak na użytkownika
- kradzież sesji
- manipulacja stroną
- brak filtracji danych

XSS (Cross-Site Scripting)

- XSS to atak „na frontend”.
  - użytkownik widzi stronę
  - ale zawiera złośliwy kod
- Może:
  - ukraść dane
  - zmienić treść strony

XSS (Cross-Site Scripting)

Na czym polega atak XSS?

A. Na przejęciu DNS i jego modyfikacji
B. Na zmianie IP klienckiego na inny wskazujący na atakującego
C. Na wstrzyknięciu złośliwego kodu wykonywanego w przeglądarce użytkownika
D. Na blokowaniu serwera i doprowadzeniu do załamania systemu

CSRF (Cross-Site Request Forgery)

- wykonanie akcji bez wiedzy użytkownika
- wykorzystanie zalogowanej sesji
- np. przelew bez zgody
- brak tokenów zabezpieczających
- atak na backend

CSRF (Cross-Site Request Forgery)

- Użytkownik jest zalogowany.
- Atakujący:
  - zmusza przeglądarkę do wysłania żądania
- System:
  - „myśli”, że to użytkownik

CSRF (Cross-Site Request Forgery)

- **GET**: Złośliwy link lub obrazek z parametrami w URL, np.
  <img src="http://bank.com/transfer.do?acct=ATTACKER&amount=1000">.

- **POST**: Formularz HTML z ukrytymi polami, który automatycznie wysyła żądanie za pomocą JavaScript:

```
<body onload="document.forms[0].submit()">
<form action="http://bank.com/transfer.do" method="POST">
<input type="hidden" name="acct" value="ATTACKER">
<input type="hidden" name="amount" value="1000">
</form>
</body>
```

- **Skutki ataku**
  - Atak CSRF może prowadzić do:
  - Zmiany danych użytkownika (np. hasła, adresu e-mail).
  - Przelewów bankowych na konto atakującego.
  - Dodania nowych użytkowników z uprawnieniami administratora w aplikacjach.

CSRF (Cross-Site Request Forgery)

Dlaczego CSRF jest możliwy?

A. Brak w sieci właściwego DNS
B. Wykorzystanie aktywnej sesji użytkownika
C. Brak IP w komputerze klienta
D. Brak właściwych ustawień routera w sieci użytkownika

Sesje użytkownika

- identyfikacja użytkownika
- cookie / token
- utrzymanie logowania
- bezpieczeństwo sesji
- wygasanie sesji

Sesje użytkownika

- Po zalogowaniu:
  - system musi „pamiętać”, kim jesteś
- To robi sesja.
- Problem:
  - przejęcie sesji = przejęcie konta
- Sesje ustala backend podczas logowania
  - Unikatowy SESID

Sesje użytkownika

Dlaczego ochrona sesji użytkownika jest kluczowa?

A. Bo przyspiesza Internet i dzięki temu apliakcja działa poprawnie
B. Bo zarządza DNS'em
C. Bo rezerwuje IP w DHCP na czas (sesję) użytkownika gwarantując stabilną pracę
D. Bo umożliwia identyfikację użytkownika w systemie

Bezpieczeństwo bazy danych

- kontrola dostępu
- walidacja danych
- zapytania parametryzowane
- backup
- ochrona przed SQL Injection

Bezpieczeństwo bazy danych

- Baza danych to „skarbiec”.
- Jeśli ktoś się do niej dostanie:
  - ma wszystko
- Dlatego:
  - walidacja danych
  - brak bezpośredniego dostępu

Bezpieczeństwo bazy danych

Która technika chroni przed SQL Injection?

A. DNS (pełni podstawową ochronę dla baz danych)
B. Routing, zabezpiecza przed dostaniem się intruza do systemu bazy danych
C. Zapytania parametryzowane (prepared statements)
D. DHCP (właściwie zarządza adresacją sieciową blokując działanie intruzów)

Aktualizacje i patchowanie

- poprawki bezpieczeństwa
- aktualizacja systemów
- usuwanie podatności
- automatyzacja
- utrzymanie systemu

Aktualizacje i patchowanie

- System bez aktualizacji = system podatny.
  - większość ataków wykorzystuje znane błędy
- Dlatego:
  - aktualizacje są kluczowe
  - poprawki błędów systemowych są normą

Aktualizacje i patchowanie

Dlaczego aktualizacje systemu są ważne?

A. Usuwają znane podatności bezpieczeństwa
B. Aktualizują system przez co przyspieszają Internet
C. Zmieniają IP dostosowując do aktualnych wymogów
D. Poprawiają DNS w kwestii wpisów i identyfikacji hostów

Najczęstsze błędy użytkowników

- słabe hasła
- brak 2FA
- klikanie w nieautoryzowane linki
- brak świadomości
- ignorowanie ostrzeżeń

Najczęstsze błędy użytkowników

- Największy problem:
  - człowiek
- Nie system.
  - „Kliknij tutaj. Okazja!”
  - „Twoje konto zablokowane”
  - „Mamy Cię! Jak nie chcesz rozgłosu kliknij.”
  - „Twoja paczka nie utknęła. Trzeba dopłacić”
  - „Zgłosiłem Twój nr. Telefonu do konkursu. Wygraliśmy!”

Najczęstsze błędy użytkowników

Który czynnik najczęściej prowadzi do naruszenia bezpieczeństwa?

A. Frontend aplikacji
B. System serwera
C. Baza danych
D. Błąd użytkownika

AI w cyberatakach

- automatyzacja ataków
- generowanie phishingu
- analiza danych ofiary
- personalizacja wiadomości
- skalowanie ataków

AI w cyberatakach

- Kiedyś phishing był „masowy i słaby”.
- Dziś AI potrafi:
  - napisać idealnego maila
  - dopasowanego do osoby
  - bez błędów językowych
- To powoduje:
  - trudniej wykryć atak

AI w cyberatakach

Jak AI zwiększa skuteczność phishingu?

A. Przyspiesza działanie w Internecie
B. Zmienia zapisy w DNS
C. **Tworzy bardziej realistyczne i spersonalizowane wiadomości**
D. Podmienia i markuje IP

Deepfake

- fałszywe nagrania
- manipulacja wizerunkiem
- podszywanie się pod osoby
- wykorzystanie AI
- zagrożenie dla firm

Deepfake

- Deepfake = ktoś „wygląda i brzmi jak ktoś inny”.

Przykład:

- łatwiej zastosować socjotechnikę
- „prezes” prosi o przelew
- pracownik wierzy

Deepfake

- Dlaczego deepfake jest niebezpieczny?

A. Spowalnia system operacyjny
B. Pozwala podszyć się pod zaufaną osobę
C. Zmienia dostęp do Sieci globalnej
D. Usuwa dane z baz danych w sposób automatyczny

Automatyczne ataki (boty)

- boty wykonują ataki
- brute-force
- skanowanie systemów
- masowe działania
- brak udziału człowieka

Automatyczne ataki (boty)

- Ataki dziś:
  - nie są ręczne
  - tysiące prób na sekundę
  - automatyczne łamanie haseł
  - automatyczne zdalne sprawdzanie systemów
  - ochrona profilaktyczna
    - Szyfrowanie
    - Logowanie 2FA

Automatyczne ataki (boty)

Dlaczego ataki botów są skuteczne?

A. **Mogą wykonywać tysiące operacji automatycznie**
B. Są wolniejsze i precyzyjniejsze
C. Zależne od użytkownika i jego działania w systemie operacyjnym
D. Wymagają dostępu do zapisów DNS

AI w obronie systemów

- wykrywanie anomalii
- analiza logów
- identyfikacja ataków
- automatyczna reakcja
- systemy SIEM (Security Information and Event Management)

AI w obronie systemów

- AI to nie tylko zagrożenie.
- Systemy typu IDS z AI może wykryć:
  - nietypowe logowanie
  - dziwne zachowanie
- szybciej niż człowiek bo automatycznie

AI w obronie systemów

Jak AI pomaga w bezpieczeństwie systemów?

A. Przyspiesza działanie karty sieciowej w Internecie
B. Odpowiednio zmienia adresację IP dla klienta
C. Ukrywa ślady po działaniu klienta w DNS
D. Wykrywa nietypowe zachowania i potencjalne ataki

Zasada „Zero Trust”

- brak zaufania domyślnego
- weryfikacja każdego dostępu
- kontrola użytkownika
- kontrola urządzeń
- ciągłe monitorowanie

Zasada „Zero Trust”

- Zero Trust = „nie ufaj nikomu”
  - nawet użytkownikowi w systemie
- Każda akcja:
  - musi być sprawdzona
  - weryfikacja treści informacji odebranej (aspekt techniczny – np. odnośniki)
  - sprawdzanie wiarygodności odebranej wiadomości (logiczny sens akcji – np. konsekwencje rozpoczętych procesów: odebranie paczki)

Zasada „Zero Trust”

Co oznacza podejście Zero Trust?

A. Zaufanie wszystkim użytkownikom
B. Logowanie się w systemach z odnośników bez weryfikacji
C. Weryfikację każdego dostępu niezależnie od lokalizacji
D. Obsługa zaufanych systemów z darmowych Hot Spotów

Minimalizacja dostępu

- zasada najmniejszych uprawnień
- tylko potrzebne prawa
- ograniczenie ryzyka
- kontrola użytkowników
- zarządzanie rolami

Minimalizacja dostępu

- Użytkownik powinien mieć tylko tyle uprawnień, ile potrzebuje do normalnej pracy
  - nie więcej, nie mniej
- Dlaczego?
  - mniejsze ryzyko ataku
  - mniejsze ryzyko utraty praw dostępu do danych

Minimalizacja dostępu

Dlaczego ograniczamy uprawnienia użytkowników?

A. Takie działanie przyspiesza pracę systemu
B. Bo nie każdego lubimy tak samo
C. Zmniejszamy przez to ilość pracy administratorom systemowym
D. Zmniejsza ryzyko nieautoryzowanego dostępu

Bezpieczne hasła

- długość hasła
- złożoność
- unikalność
- menedżery haseł
- brak powtarzalności

Bezpieczne hasła

- Hasło powinno być:
  - długie
  - unikalne
- Najlepsza praktyka:
  - menedżer haseł

Bezpieczne hasła

Która cecha najlepiej zwiększa bezpieczeństwo hasła?

A. **Długie i unikalne dla każdej usługi**
B. Krótkie i łatwe do zapamiętania- to przyśpiesza logowanie
C. To samo wszędzie – bardzo wygodne rozwiązanie
D. Zapisane w przeglądarce – korzystne z wielu względów

Aktualizacje systemów

- poprawki bezpieczeństwa
- usuwanie luk
- automatyczne aktualizacje
- nowe wersje
- ciągłe utrzymanie

Aktualizacje systemów

- Nieaktualny system:
  - łatwy cel
  - większość ataków wykorzystuje stare błędy
  - brak aktualizacji umożliwia zastosowanie scenariusza ataku
  - złamane systemy są potencjałem przy atakach kaskadowych
  -

Aktualizacje systemów

- Nieaktualny system:
  - łatwy cel
  - większość ataków wykorzystuje stare błędy
  - brak aktualizacji umożliwia zastosowanie scenariusza ataku
  - złamane systemy są potencjałem przy atakach kaskadowych (pivoting/proxying)

Aktualizacje systemów

Dlaczego brak aktualizacji jest zagrożeniem?

A. Pozostawia znane podatności otwarte
B. Dane aktualizacji spowalniają system dość znacznie
C. Przy pobieraniu aktualizacji system otwiera porty i wtedy atakujący jest w stanie działać
D. Bo ciężko zarejestrować wtedy komputer w sieci

Bezpieczeństwo sieci

- firewall
- segmentacja sieci
- monitoring
- kontrola ruchu
- ochrona infrastruktury

Bezpieczeństwo sieci

- Sieć to pierwsza linia obrony.
  - firewall = filtr ruchu
  - Filtry pakietów – warstwa sieci
  - Filtry aplikacyjne – warstwa aplikacji
  - Filtry adaptacyjne - hybryda

Bezpieczeństwo sieci

Jaką rolę pełni firewall?

A. Przechowuje dane o atakach
B. Kontroluje i filtruje ruch sieciowy
C. Zarządza dostępem do danych użytkownika
D. Tworzy bezpieczne hasła i realizuje uwierzytelnienie

Bezpieczeństwo użytkownika

- świadomość zagrożeń
- ostrożność
- weryfikacja źródeł
- edukacja
- unikanie ryzyka

Bezpieczeństwo użytkownika

- Najlepsze zabezpieczenie:
  - świadomy użytkownik

Bezpieczeństwo użytkownika

Co jest najważniejszym elementem bezpieczeństwa?

A. Dobrze zaprogramowany Router
B. Zabezpieczony właściwie DNS
C. Bezpieczny i bezawaryjny kabel
D. Świadomy użytkownik

Bezpieczeństwo aplikacji

- walidacja danych
- filtrowanie wejścia
- ochrona backendu
- ochrona API
- testy bezpieczeństwa

Bezpieczeństwo aplikacji

- Programista i developer musi myśleć o bezpieczeństwie.
- każde wejście = potencjalny atak
- każde wypełnienie formularza – potencjalny atak
- Interakcja z bazą danych = weryfikacja zapytań
- kod aplikacji = kompozycja zabezpieczeń (rejestracja, logowanie, walidacja, weryfikacja,…)

Bezpieczeństwo aplikacji

Dlaczego monitoring systemu jest ważny?

A. **Pozwala wykryć i analizować incydenty bezpieczeństwa**
B. Automatycznie zapobiega dostaniu się kodu szkodliwego
C. Modyfikuje IP w razie włamania do systemu
D. Całkowicie zapobiega atakom z Internetu

Najczęstsze błędy

- brak aktualizacji
- brak zabezpieczeń
- brak testów
- ignorowanie zagrożeń
- brak polityk bezpieczeństwa

Najczęstsze błędy

- Najczęstszy problem:
  - „nas to nie dotyczy”
  - „nic takiego nie mamy w sieci żeby stanowiło to potencjał dla hackera”
  - „nasza sieć jest zabezpieczona na zaś”
  - „mamy super nowy sprzęt od zabezpieczeń”
  - „tu jest szczelniej niż w Pentagonie”

Najczęstsze błędy

Który błąd jest najczęstszy w sieciach?

A. Zbyt dużo zabezpieczeń i dlatego za wolno to wszystko działa
B. Ignorowanie zagrożeń i brak procedur
C. Instalacja nowego oprogramowania bez analizy bezpieczeństwa
D. Otwieranie sieci dla nowych kooperantów

Podsumowanie bezpieczeństwa

- zagrożenia są realne
- technologia + użytkownik
- proces ciągły
- AI jako wsparcie i zagrożenie
- świadomość kluczem

Podsumowanie bezpieczeństwa

- Bezpieczeństwo to nie produkt.
  - **to proces!**

Podsumowanie bezpieczeństwa

Co najlepiej opisuje bezpieczeństwo IT?

A. Jednorazowa konfiguracja
B. Instalacja programu antywirusowego
C. Ciągły proces zarządzania ryzykiem
D. Aktualizacja systemu