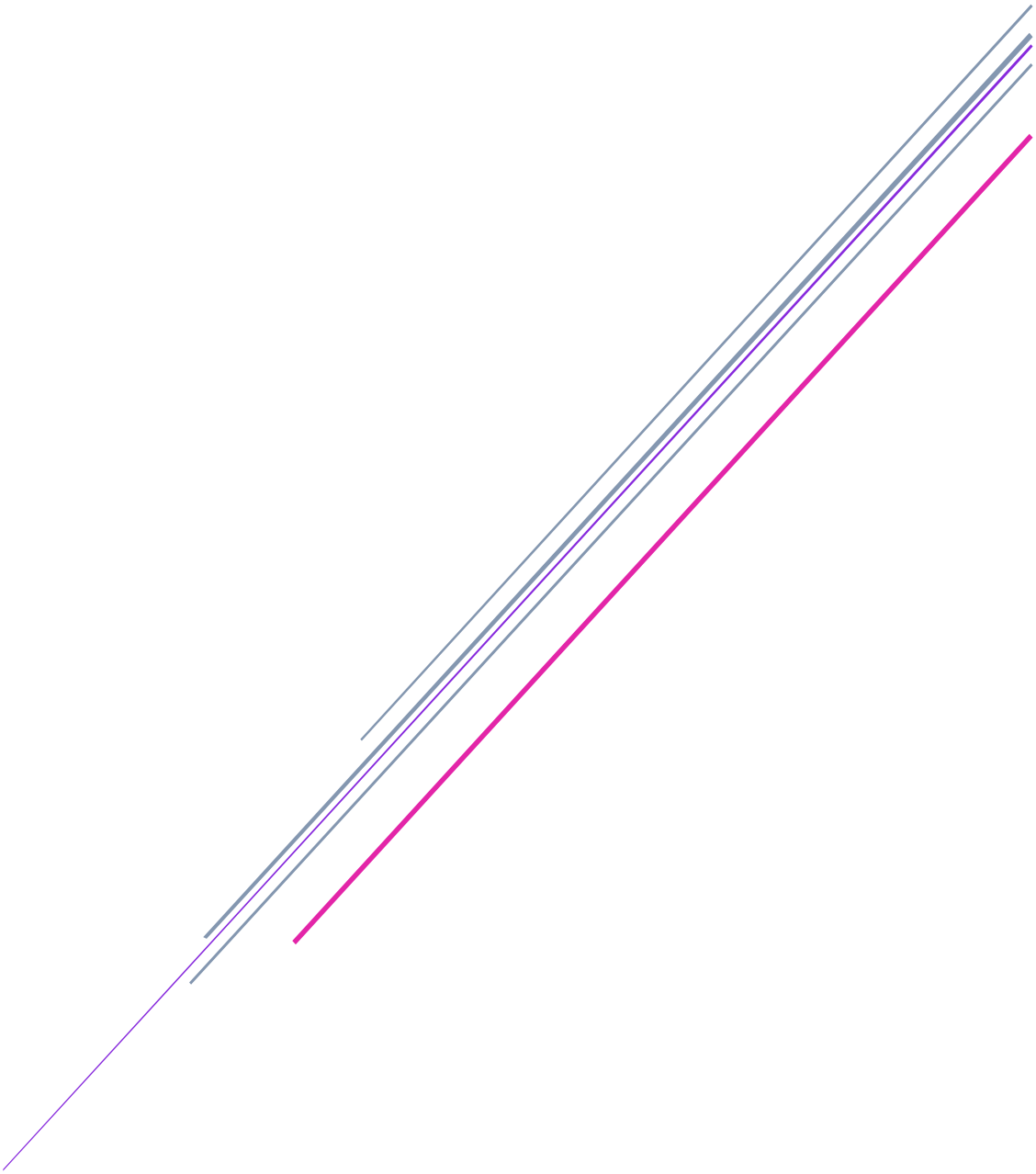
SIGURNOST U MREŽNOM PROGRAMIRANJU DRUŠTVENIH MREŽA

SEMINARSKI RAD



Nika Bevanda 3.C
šk. god. 2024./25.

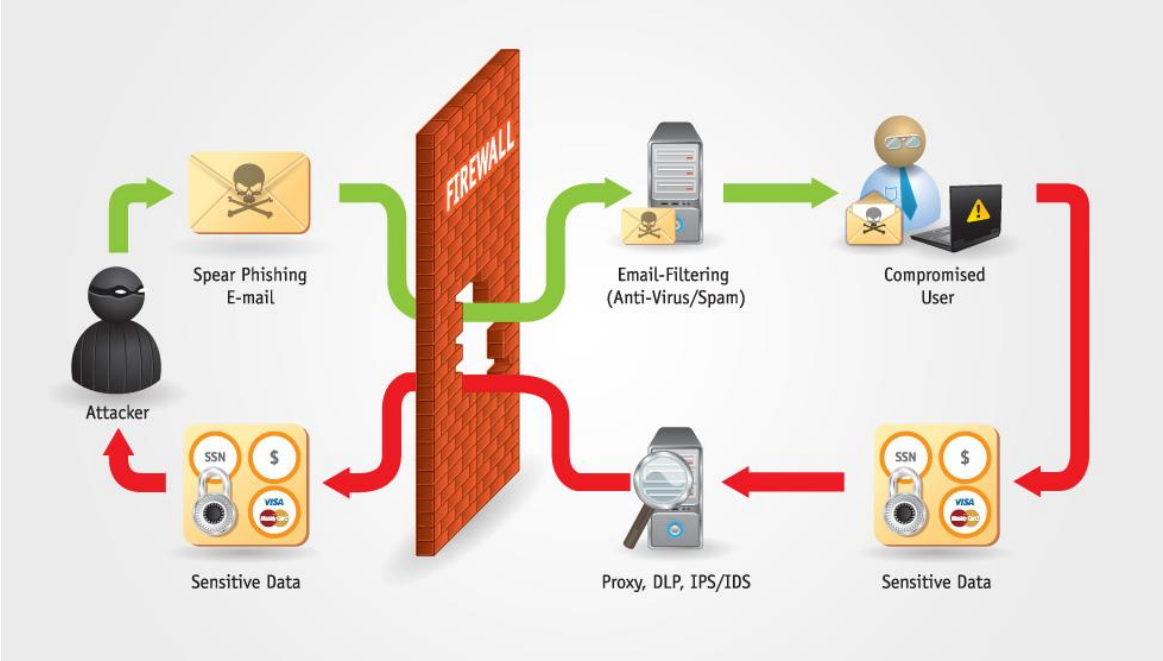
SADRŽAJ

GLAVNE PRIJETNJE DRUŠTVENIM MREŽAMA

Sigurnost u mrežnom programiranju društvenih mreža odnosi se na zaštitu podataka, aplikacija i korisnika od različitih prijetnji kod velike razmjene osjetljivih informacija putem internetskih platformi.

Glavne prijetnje su:

* **Neovlašteni pristup korisničkim računima** - Phishing napadi, slabe lozinke ili ponovna uporaba istih lozinki.



* **Curenje podataka** - Hakiranje baza podataka koje sadrže privatne informacije korisnika.

* **Malware i zlonamjerni linkovi** - Dijeljenje zlonamjernih veza putem postova ili privatnih poruka.

* **Lažni profili i botovi** - Automatizirani ili lažni računi za manipulaciju sadržajem i širenje dezinformacija.

* **Denial-of-Service (DoS) napadi** - Napadi usmjereni na prekid rada platforme.

SIGURNOSNE MJERE U RAZVOJU DRUŠTVENIH MREŽA

Korisnički podaci

A. **Šifriranje podataka:**
   - U prijenosu - TLS/SSL protokoli za osiguranje komunikacije između klijenata i servera.
   - U pohrani – AES (Advanced Encryption Standard) šifriranje za osjetljive podatke poput lozinki i osobnih informacija.

B. **Sigurnosna pravila lozinki:**
   - Snažne lozinke (min. duljina, mješavina znakova) i obvezna promjena lozinki nakon curenja podataka.
   - Upotreba hash algoritama poput bcrypt za pohranu lozinki.

C. **Dvofaktorska autentifikacija:**
   - Kombinacija lozinke i jednokratnih kodova putem aplikacija, SMS-a ili e-pošte.

D. **Kontrola pristupa:**
   - Uvođenje granularnih dozvola za korisnike, administratora i sustave.

Infrastruktura

- **Ograničenje API pristupa:**

  Upotreba sigurnih API (Application Programming Interfaces) ključeva i ograničavanje zahtjeva prema IP adresama ili razinama autorizacije.

- **Detekcija i prevencija DDoS napada:**

  Upotreba mreža za isporuku sadržaja i alata za filtriranje zlonamjernog prometa.

- **Redovito ažuriranje softvera:**

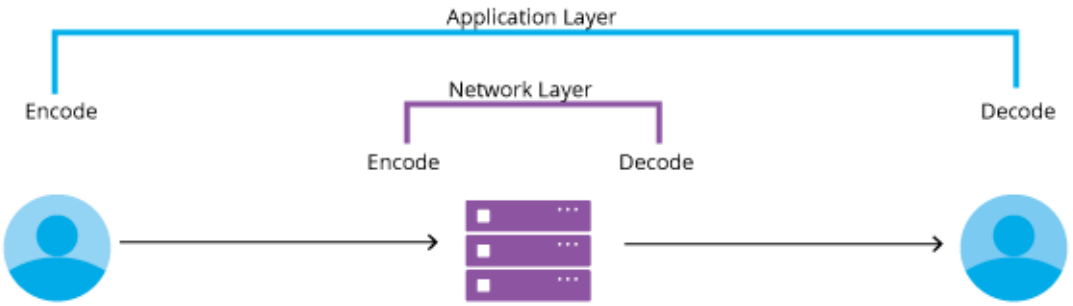
  Primjena zakrpa za poznate ranjivosti u kodu i serverima.

- **Praćenje aktivnosti servera:**

  Implementacija alata za praćenje i analizu sumnjivih aktivnosti.

Komunikacija

1. **End-to-end šifriranje (E2EE):**
    - Za privatne poruke i osjetljive komunikacije između korisnika.
    - Implementacija standarda poput Signal protokola.



2. **Ograničenje dijeljenja podataka:**
    - Jasne postavke privatnosti za korisnike i algoritmi za minimizaciju dijeljenja osjetljivih podataka s trećim stranama.

3. **Detekcija zlonamjernih sadržaja:**
    - Automatska analiza linkova i datoteka koje korisnici dijele pomoću sustava poput VirusTotal.

Zaštita od zlonamjernih aktivnosti

A. **Validacija korisničkog sadržaja:**

- Sprečavanje unosa koda putem unosa korisnika.

B. **Otkrivanje lažnih profila i botova:**

- Primjena strojnog učenja za identifikaciju neautentičnih računa.

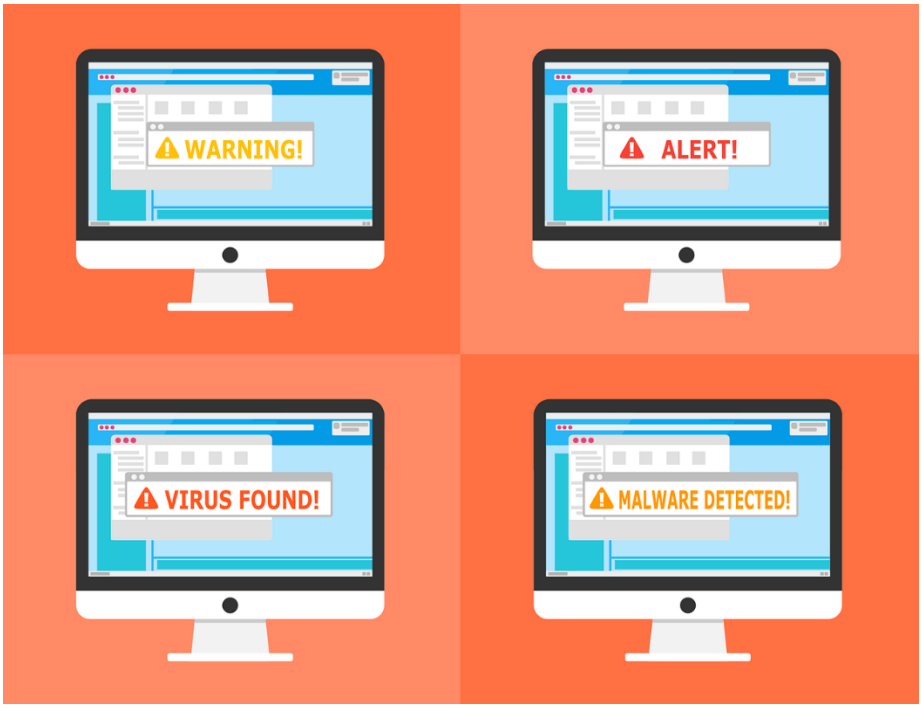
C. **Sustav upozorenja:**

- Obavijesti korisnicima o pokušajima prijave s novih uređaja ili lokacija.

Transparentnost i povjerenje

A. **Izvještaji o sigurnosnim incidentima:**

- Brzo obavještavanje korisnika o probojima i preporuke za minimizaciju štete.



B. **Alati za kontrolu privatnosti:**

- Omogućiti korisnicima da odrede koje informacije žele podijeliti i s kim.

C. **Redoviti auditi sigurnosti:**

- Vanjske provjere sigurnosnih praksi i revizije koda.

BUDUĆNOST ZAŠTITE NA DRUŠTVENIM MREŽAMA

Tehnološki razvoj, poput umjetne inteligencije za prepoznavanje prijetnji, blockchain za veću privatnost i transparentnost podataka, te kryptografske metode za bolju zaštitu identiteta korisnika, upućuju na poboljšanje sigurnosti na društvenim mrežama.

Ali to ne znači da njihovo napredovanje tu staje. Kako se sigurnost razvija, tako prijetnje i napadi evoluiraju te zbog toga društvene mreže moraju stalno nadograđivati svoje sigurnosne sustave.

A ono što svakako će uvijek pružati određenu sigurnost je korištenje jakih lozinki, oprez prilikom prihvaćanja prijateljskih zahtjeva i poznavanje opasnosti od različitih online prijetnji.

LITERATURA

https://repozitorij.foi.unizg.hr/islandora/object/foi:2959

https://cso.cyberhandbook.org/sr/topics/staying-safe/bezbednost-drustvenih-mreza

https://repozitorij.vup.ftrr.hr/islandora/object/vup:2000