STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Sociálne siete**

aspekty a ohrozenia bezpečnosti na nich

**Sofiia Kuchko**

2024

Obsah

Obsah 2

Anotácia 3

1 Úvod do bezpečnosti sociálnych sietí 4

2 Štruktúra a ochrana sociálnych sietí 5

2.1 Klientské komponenty 5

2.2 Komponenty servera 5

2.3 Sieťová ochrana 5

2.4 Autentifikácia a autorizácia 5

2.5 Ochrana osobných údajov 6

3 Bezpečnostné ohrozenia v sociálnych sieťach 7

3.1 Phishing 7

3.2 Škodlivý softvér 7

3.3 Kyberšikana 7

3.4 Únik osobných údajov 7

3.4.1 Únik osobných údajov na sociálnej sieti Facebook. 7

3.5 Spam a nežiaduca reklama 8

3.6 Sociálne inžinierstvo 8

4 Overovanie a autorizácia v sociálnych sieťach: technické aspekty 9

4.1 Používanie hesiel 9

4.2 Dvojfaktorová autentifikácia (2FA) 9

4.3 Biometrické metódy autentifikácie 9

5 Ilustrácie, tabuľky, rovnice 10

5.1 Ilustrácie 10

5.2 Tabuľky 10

5.3 Zdrojový kód programu 11

5.4 Rovnice, vzorce 11

6 Záver 12

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla) 13

Prílohy (štýl Nadpis Kapitoly, bez čísla) 14

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla) 14

Príloha B – <názov prílohy> 14

Príloha C – <názov prílohy> 14

Anotácia

**Annotation**

1. Úvod do bezpečnosti sociálnych sietí

V dnešnom svete zohrávajú sociálne siete obrovskú úlohu v živote miliónov ľudí po celom svete. Stali sa hlavným spôsobom komunikácie, zdieľania dôležitých informácií, vytvárania a šírenia obsahu a udržiavania sociálnych kontaktov. Keďže sú ľahko dostupné a používateľsky jednoduché, najmä na mobilných zariadeniach, sociálne médiá sa stali pevnou súčasťou nášho každodenného života.

Spolu s ich šírením a rastúcim počtom používateľov sa však objavili aj bezpečnostné ohrozenia, ktoré môžu spôsobiť vážne škody jednotlivým používateľom aj samotným platformám sociálnych sietí. Tieto hrozby siahajú od kyberšikany a kyberstalkingu až po krádež osobných údajov, šírenie vírusov a phishingové útoky.

Cieľom tohto projektu je poskytnúť čitateľovi lepšie pochopenie bezpečnosti sociálnych sietí z technického hľadiska. Zameriame sa na rozbor hlavných hrozieb a pozrieme sa na rôzne metódy a prístupy na ich prekonanie.

1. Štruktúra a ochrana sociálnych sietí

Sociálne siete sú komplexné informačné systémy, ktoré zahŕňajú rôzne komponenty a služby určené na interakciu používateľov a ukladanie a spracovanie údajov používateľov. V tejto kapitole sa budeme zaoberať hlavnými zložkami štruktúry sociálnych sietí a metódami bezpečnostného zabezpečenia používanými na rôznych úrovniach.

* 1. Klientské komponenty

Klientské komponenty sociálnych sietí sú softvérové alebo webové rozhrania, ktoré používatelia používajú na prístup k službám. Môžu to byť mobilné aplikácie, webové prehliadače alebo počítačové programy. Na tejto úrovni je dôležité zabezpečiť bezpečnosť vrátane ochrany proti cross-site útokom (XSS), zachytávaniu údajov (MITM) a malvéru.

* 1. Komponenty servera

Serverové komponenty predstavujú serverový softvér, ktorý spracováva požiadavky klientov, poskytuje ukladanie údajov a spravuje obchodnú logiku aplikácií. Bezpečnosť na tejto úrovni si vyžaduje ochranu serverov pred útokmi DDoS, ochranu databáz pred neoprávneným prístupom a monitorovanie bezpečnosti na úrovni jednotlivých aplikácií.

* 1. Sieťová ochrana

Sieťová ochrana zahŕňa opatrenia na ochranu pred vonkajšími útokmi, ako je filtrovanie prevádzky, nastavenie firewallov, používanie virtuálnych privátnych sietí (VPN) a používanie šifrovania dát na transportnej vrstve (TLS/SSL).

* 1. Autentifikácia a autorizácia

Autentifikácia a autorizácia zohrávajú dôležitú úlohu pri zabezpečení sociálnych sietí. Je potrebné zaviesť silné metódy autentifikácie, ako sú silné heslá, dvojfaktorová autentifikácia a biometrická autentifikácia. K tejto téme sa vrátime neskôr a bližšie sa jej budeme venovať.

* 1. Ochrana osobných údajov

Ochrana údajov v sociálnych médiách spočíva v šifrovaní údajov v stave uloženia a pri prenose, správnom riadení prístupu k údajom, zálohovaní údajov a monitorovaní činnosti používateľov s cieľom odhaliť podozrivé aktivity.

Pochopenie a správna implementácia zabezpečenia na rôznych úrovniach štruktúry sociálnych sietí je dôležitým aspektom na zaistenie bezpečnosti používateľov a ochranu ich osobných údajov. S neustálym vývojom technológií a vznikom nových hrozieb je však dôležité neustále aktualizovať a zlepšovať bezpečnostné systémy, aby spĺňali súčasné normy a požiadavky.

1. Bezpečnostné ohrozenia v sociálnych sieťach

Sociálne médiá sú úrodnou pôdou pre rôzne bezpečnostné hrozby, ktoré môžu poškodiť nielen jednotlivých používateľov, ale aj celú platformu. V tejto kapitole budeme analyzovať a klasifikovať hlavné hrozby, ktorým čelia sociálne siete, a pozrieme sa na spôsoby, ako im predchádzať.

* 1. Phishing

Phishingové útoky sú pokusy o podvod, pri ktorých sa útočníci vydávajú za dôveryhodné osoby alebo organizácie s cieľom získať prístup k osobným údajom používateľov, ako sú heslá, čísla kreditných kariet a iné dôležité údaje. Phishingové útoky sa môžu uskutočňovať prostredníctvom e-mailov, príspevkov v sociálnych sieťach, webových stránok s pascami a iných kanálov.

* 1. Škodlivý softvér

Škodlivý softvér (malvér) je softvér určený na poškodzovanie počítačových systémov alebo používateľov. Malvér sa môže šíriť na sociálnych sieťach prostredníctvom infikovaných odkazov, príloh správ, falošných aplikácií alebo reklám.

* 1. Kyberšikana

Kyberšikana je forma online šikanovania alebo obťažovania, pri ktorej sú používatelia sociálnych médií nútení čeliť hrozbám, urážkam, nenávistným prejavom alebo iným formám diskriminácie. Kyberšikanovanie môže mať pre obeť vážne psychické dôsledky a často vedie k zvýšeným negatívnym emóciám a depresii.

* 1. Únik osobných údajov

Únik osobných údajov je jednou z najvážnejších hrozieb pre používateľov sociálnych sietí. Môže k nim dôjsť v dôsledku nedostatočnej ochrany údajov na serveroch platformy, chýb v nastaveniach ochrany osobných údajov používateľov alebo škodlivých útokov na systém.

* + 1. Únik osobných údajov na sociálnej sieti Facebook.

Považujem za dôležité spomenúť jeden z najväčších príkladov úniku osobných údajov, ku ktorému došlo v roku 2018 v sociálnej sieti Facebook. V marci 2018 sa zistilo, že údaje viac ako 87 miliónov používateľov Facebooku boli nezákonne zhromaždené a použité na účely politickej reklamy a manipulácie. Tento únik údajov súvisel s činnosťou britskej konzultačnej spoločnosti Cambridge Analytica, ktorá získala prístup k osobným údajom používateľov Facebooku bez ich súhlasu.

Tento únik spôsobilo viacero faktorov:

1. Nedostatočné opatrenia na ochranu údajov: Facebook zaviedol do svojej platformy chybu, ktorá umožňovala aplikáciám tretích strán zhromažďovať veľké množstvo osobných údajov používateľov bez ich výslovného súhlasu. Bolo to spôsobené chybným systémom kontroly prístupu a správy údajov na platforme.

2. Nejasné zásady ochrany osobných údajov: Používateľom nebolo vždy jasné, aké údaje sa zbierajú a ako sa budú používať. Facebook mal zložité a často sa meniace zásady ochrany osobných údajov, ktoré mohli u používateľov vyvolať zmätok v otázke ochrany ich osobných údajov.

3. nedostatočná kontrola vývojárov externých spoločností: Facebook poskytol prístup k údajom svojich používateľov vývojárom externých spoločností prostredníctvom rozhrania API (aplikačné programovacie rozhranie) bez náležitej kontroly a primeraných bezpečnostných opatrení.

Tento incident poukázal na dôležitosť nielen technických opatrení na ochranu údajov, ale aj prehľadnosti, pokiaľ ide o zbieranie a používanie osobných údajov používateľov. Po tomto incidente čelila spoločnosť Facebook viacerým právnym problémom a problémom s reputáciou a bola nútená zmeniť svoje zásady a postupy ochrany údajov, aby v budúcnosti zabránila podobným incidentom.

* 1. Spam a nežiaduca reklama

Spam a nežiaduce reklamy sú bežnými problémami na sociálnych sieťach. Môžu obsahovať rušivé reklamné správy, nepravdivé informácie a odkazy na škodlivé alebo podozrivé zdroje.

* 1. Sociálne inžinierstvo

Sociálne inžinierstvo je spôsobom manipulácie s ľuďmi s cieľom získať citlivé informácie alebo vykonať určité činnosti. Môže to zahŕňať oklamanie používateľov, aby získali svoje heslá, prístup k svojim účtom alebo prezradili citlivé údaje.

1. Overovanie a autorizácia v sociálnych sieťach: technické aspekty

Tejto téme sme sa už začali venovať. V tejto kapitole sa však budeme podrobnejšie zaoberať rôznymi technickými aspektmi týchto procesov a spôsobom ich realizácie.

* 1. Používanie hesiel

Overovanie heslom je najbežnejšou metódou autentifikácie používateľov. Každý používateľ si vytvorí jedinečné heslo, ktoré sa potom uloží zašifrované v databáze. Na zvýšenie bezpečnosti sa odporúča používať zložité heslá, ktoré obsahujú kombináciu písmen, číslic a špeciálnych znakov, a pravidelne ich meniť.

* 1. Dvojfaktorová autentifikácia (2FA)

Dvojfaktorová autentifikácia pridáva ďalšiu úroveň zabezpečenia tým, že vyžaduje, aby používateľ poskytol dva typy dôkazov identity. Môže ísť o kombináciu niečoho, čo používateľ pozná (napríklad heslo), a niečoho, čo má (napríklad jednorazový kód zaslaný na mobilný telefón). Táto metóda výrazne zvyšuje bezpečnosť a chráni účet aj v prípade, že je heslo zneužité.

* 1. Biometrické metódy autentifikácie

Biometrické overovanie využíva jedinečné fyziologické a správacie charakteristiky používateľa na overenie jeho totožnosti. Môže ísť o skenovanie odtlačkov prstov, rozpoznávanie tváre, skenovanie dúhovky alebo dokonca rozpoznávanie hlasu. Biometrické metódy poskytujú vysokú úroveň zabezpečenia, pretože sa ťažšie falšujú ako heslá.

Implementácia autentifikácie a autorizácie v sociálnych sieťach je zložitý a viacvrstvový proces, ktorý si vyžaduje kombináciu rôznych metód a technológií. Je dôležité nielen zabezpečiť vysokú úroveň bezpečnosti používateľov, ale aj to, aby bol proces overovania pohodlný a intuitívny. Správne používanie moderných metód autentifikácie a autorizácie minimalizuje riziká ohrozenia účtu a chráni osobné údaje používateľov pred nezákonným prístupom

1. Ilustrácie, tabuľky, rovnice

V práci sa môžu vyskytovať okrem slovného textu aj informácie vyjadrené v obrazovej forme a symbolmi.

* 1. Ilustrácie

**Ilustrácie** sú obrázky obsahujúce **grafy**, **diagramy**, **mapy**, **schémy** a pod. Nie je potrebné rozlišovať rozličné typy ilustrácií, stačí, ak sa všetky označia ako „Obrázok”. Všetky ilustrácie musia byť očíslované súvislým radom číslic v celej práci a musia mať titulky (názov obrázku) pri každom obrázku. Text titulku musí byť pochopiteľný aj bez kontextu. Majú sa zaradiť bezprostredne za textom, kde sa spomínajú po prvýkrát (najlepšie na tej istej strane). Obrázok by mal byť podľa možnosti centrovaný. Pri odkazovaní na daný obrázok v texte použijeme odkaz uvedený v zátvorke (napr. Obr. 1).



Obr. 1 Názov obrázka (štýl Popis, Popiska-Caption)

* 1. Tabuľky

Tabuľky prezentujú myšlienky a tvrdenia popisované v práci. Akýkoľvek tabuľkový materiál, ktorý sa skladá z viac než štyroch alebo piatich riadkov, by mal byť spracovaný do formy tabuľky. Popis a záhlavie tabuľky má byť zrozumiteľné samostatne bez odkazu na text. Záhlavia majú vyjadrovať druh veličiny a typy jednotiek vo forme „veličina/jednotka”, je potrebné používať rovnaké symboly a skratky ako v texte. Každá tabuľka musí mať poradové číslo a titulok, umiestnený zvyčajne nad tabuľkou. Tabuľka by mala mať rovnakú orientáciu, ako text práce.

Tab. 1 Názov tabuľky (štýl Popis, Popiska-Caption)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1.A | 1.B | 1.C | 1.D |
| prezentácie | 10 | 12 | 13 | 11 |
| videá | 7 | 4 | 6 | 3 |
| počítačové hry | 5 | 6 | 3 | 4 |
| blogy | 6 | 8 | 7 | 8 |
| postery | 4 | 3 | 5 | 6 |

* 1. Zdrojový kód programu

Na zápis zdrojového kódu programu použijeme štýl kód (písmo Courier New 11, zarovnanie vľavo, orámovanie s tieňom).

viem hľadajCestu

  kým [farbabodu <> "čierna] [vz 1]

  do 1 vp 90

  kým [farbabodu <> "červená] [

   vp 90 do 1

   ak farbabodu = "čierna [

    vz 1 vl 90 do 1

    ak farbabodu = "čierna [vz 1 vl 90]

   ]

   čakaj 1

  ]

koniec

* 1. Rovnice, vzorce

Rovnice sa uvádzajú v strede riadka, vysvetlivky symbolov na začiatku riadku. Vysvetlivky symbolov sa uvádzajú od začiatku riadka. Ak je v práci viac vzorcov, uvádzame číslo vzorca do okrúhlych zátvoriek bez medzier umiestnených na pravom konci riadka. Pre písanie fyzikálnych veličín a matematických premenných sa používa kurzíva. Používame sústavu jednotiek SI (ISO 31 a ISO 1001). Pri písaní rovníc používame **editor rovníc (musíme ho mať nainštalovaný)**.

1. Záver

Záver obsahuje vecné závery, sumarizáciu, vlastný prínos alebo pohľad autora, odporúčania pre prax (výučbu). Záver je uvedený na maximálne 1 stranu.

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla)

Všetky dokumenty, ktoré v práci použijete, je potrebné zoradiť do zoznamu pozostávajúceho z  bibliografických odkazov, ktorý označujeme **Zoznam použitej literatúry**. Pre tvorbu zoznamov použitej literatúry platia štandardy. Cieľom je, aby zo zoznamu použitej literatúry bolo možné jasne identifikovať použitý zdroj a aby ho bolo možné bez ťažkostí opäť vyhľadať.

Hlavným zdrojom údajov pre tvorbu bibl. odkazov je **titulný list** (tzn. prvý list v knihe, kde sú uvedené údaje o názve autorovi atď.), príp. jeho rub. Odkazy sa môžu týkať knižných, časopiseckých a iných zdrojov informácií (zborníky z konferencií, patentové dokumenty, normy, odporúčania, kvalifikačné práce, osobná korešpondencia a rukopisy, odkazy cez sprostredkujúci zdroj, elektronické publikácie), ktoré boli v práci použité.

**Technika citovania** určuje spôsob, akým označujeme citácie v dokumente, pričom podľa normy (pozri STN ISO 690) existuje viacero spôsobov citovania. Pri metóde **číselných citácií** sa v zozname bibliografických odkazov každé citované dielo uvádza v tom poradí, v akom bolo uvedené a číslované v texte. Číslované odkazy v texte sú uvedené v zátvorkách [3] a odkazujú na dokumenty v takom poradí, v akom sa citujú po prvýkrát. Nasledujúce citácie dostávajú také isté číslo, ako má prvá citácia. Ak sa citujú osobitné časti dokumentu, môžu sa za číslom citácie uviesť čísla strán.

**Príklad zoznamu použitej literatúry:**

1. KALAŠ, Ivan – BLAHO, Andrej: *Tvorivá informatika. 1. zošit z programovania.* Bratislava: SPN - Mladé letá, 2007. 48. s. ISBN 80-10-01723-2
2. CIMBALA, Roman – BALOGH, Jozef – DŽMURA, Jaroslav: Diagnostika výkonových transformátorov s využitím prvkov umelej inteligencie 1. In: *Elektrotechnický magazín ETM*. roč. 14, č. 1 (2004), s. 8-9.
3. Kolektív autorov: *Štátny vzdelávací program*. [online] Bratislava: ŠPU v Bratislave, 2008. Aktualizované 14.2.2010 [cit. 2010-02-17]. Dostupné na internete: <http://new.statpedu.sk/sk/filemanager/download/987>
4. Elektronické diplomové a dizertačné práce SR: ETD SK. [online]. Košice : ETD SK, 2004. Aktualizované 14-2-2005 [cit 2005-03-10]. Dostupné na internete: <http://www.etd.sk/>.
5. KATUŠČÁK, Dušan: *Ako písať záverečné a kvalifikačné práce*. Nitra: Enigma, 2004. 162 s. il. ISBN 80-89132-10-3

Prílohy (štýl Nadpis Kapitoly, bez čísla)

Zoznam príloh záverečnej práce:

* Príloha A – CD médium
* Príloha B – <názov prílohy>
* Príloha C – <názov prílohy>

Táto časť záverečnej práce obsahuje zoznam všetkých príloh. Číslovanie strán príloh nadväzuje na číslovanie strán v hlavnom texte.

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla)

Priložené CD médium **povinne** obsahuje text záverečnej práce vo formáte PDF. CD môže obsahovať edukačný hypertext, metodické listy, dotazníky a ukážky projektov atď. CD médium zabalené do papierového obalu sa vlepí na vnútornú stranu zadnej obálky záverečnej práce.

Príloha B – <názov prílohy>

<popis prílohy>

Príloha C – <názov prílohy>

<popis prílohy>