STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Sociálne siete**

aspekty a ohrozenia bezpečnosti

**Sofiia Kuchko**

2024

Obsah

Anotácia 3

Úvod do bezpečnosti sociálnych sietí 4

1 Štruktúra a ochrana sociálnych sietí 5

1.1 Klientské a serverové komponenty 5

1.2 Sieťová ochrana 5

1.3 Ochrana osobných údajov 5

2 Bezpečnostné ohrozenia v sociálnych sieťach 6

2.1 Malware 6

2.2 Sociálne inžinierstvo 6

2.3 Únik osobných údajov 7

2.3.1 Únik osobných údajov na sociálnej sieti Facebook. 7

3 Overovanie a autorizácia v sociálnych sieťach: technické aspekty 9

3.1 Používanie hesiel 9

3.2 Dvojfaktorová autentifikácia (2FA) 9

3.3 Biometrické metódy autentifikácie 9

4 Produkt a jeho tvorba 11

4.1 Cieľová skupina 11

4.2 Farby 12

4.3 Text a jeho obsah 12

4.4 Ilustrácie 13

5 Záver 14

Zoznam použitej literatúry 15

Anotácia

Práca je venovaná analýze bezpečnostných aspektov v sociálnych sieťach. V kontexte rastúcej popularity sociálnych médií a hrozieb spojených s používaním online platforiem skúmam kľúčové komponenty štruktúry sociálnych sietí a metódy ich ochrany na rôznych úrovniach. Špeciálna pozornosť sa venuje ochrane osobných údajov, predchádzaniu úniku informácií a analýze hlavných hrozieb, ako sú malvéry a sociálna inžinieria. Práca tiež popisuje technické metódy autentifikácie a autorizácie používateľov v sociálnych sieťach, vrátane použitia hesiel, dvojfaktorovej autentifikácie a biometrických údajov. Okrem toho popisujem proces tvorby produktu, v tomto prípade plagátu, s dôrazom na výber cieľovej skupiny, farebnú schému, text a ilustrácie.

**Annotation**

This work is focused on the analysis of security aspects in social networks. In the context of the growing popularity of social media and the dangers associated with the use of online platforms, I examine the key components of the social networking structure and the methods of protecting it at different levels. Special attention is paid to data privacy, information leakage prevention, and analysis of major threats such as malware and social engineering. The thesis also describes technical methods of user authentication and authorization in social networks, including the use of passwords, two-factor authentication and biometrics. In addition, I describe the process of creating a product, in this case a poster, with an emphasis on target audience selection, color scheme, text, and illustrations.

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.



Obrázok č. Social Media. Zdroj: < https://www.pinterest.com/pin/348888302385127084/ >

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 a serverové komponenty

1. 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.
2. 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. 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. Malware

Malvér predstavuje všetky formy škodlivého softvéru, vrátane trójskych koní, ransomware, vírusov, červov a bankového malvéru. Spoločným rysom všetkých týchto typov je nekalý úmysel ich tvorcov alebo prevádzkovateľov.

Rozpoznanie malvéru môže byť pre bežného používateľa náročné, pretože je ťažké rozlíšiť medzi bezpečnými a škodlivými súbormi. Bezpečnostné riešenia využívajú rozsiahle databázy škodlivých vzoriek a rôzne technológie na ochranu pred novými hrozbami.

Malvér je často šírený pomocou bezpečnostných zraniteľností v systémoch, neaktualizovaných softvérov alebo prostredníctvom e-mailových príloh, ktoré môžu obsahovať škodlivý kód. Ľudský faktor zostáva jedným z najslabších miest v bezpečnostnom reťazci, keďže do systému môže škodlivý kód preniknúť jednoduchým kliknutím na zlý odkaz či prílohu v e-maile.[1]

* 1. Sociálne inžinierstvo

Sociálne inžinierstvo je spôsob manipulácie ľudí s cieľom získať od nich informácie dôverného charakteru alebo prinútiť ich k vykonaniu požadovanej činnosti.

Tento spôsob útokov na organizácie a získavania informácií býva veľmi úspešný. Aj napriek tomu, že si nevyžaduje takmer žiadne špeciálne technické znalosti a technologické prostriedky. Sociálne inžinierstvo sa svojimi metódami a praktikami snaží využiť hlavne faktory, ktoré ovplyvňujú ľudské správanie a rozhodovanie.[2] Príkladmi sociálneho inžinierstva môžu byť phishingové útoky alebo kyberšikanovanie.

1. 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.[3],[4]
2. Kyberšikanovanie predstavuje formu online šikany, charakterizovanú nútením používateľov sociálnych médií čeliť rôznym formám nebezpečenstva, vrátane hrozieb, urážok, nenávistných prejavov a formy diskriminácie. Tento jav môže mať vážne psychické dôsledky pre postihnutých, často vieduc k negatívnym emóciám a depresii. Aj keď kyberšikanovanie nie je priamo technickou hrozbou, je kritickým aspektom bezpečnosti v online prostredí, nakoľko predstavuje riziko pre psychologické a emocionálne blaho používateľov.[5]
   1. Únik osobných údajov

Únik údajov predstavuje incident, kedy dochádza k neoprávnenemu vylúčeniu alebo získaniu dôverných informácií z akéhokoľvek systému bez vedomia alebo súhlasu ich vlastníka. Tento jav postihuje organizácie rôznych veľkostí, vrátane malých a veľkých firiem, subjektov štátnej správy a neziskových organizácií, a môže zahŕňať osobné údaje ako rodné čísla, bankové účty, finančné informácie, zdravotné údaje, duševné vlastníctvo a záznamy o zákazníkoch. Úniky údajov môžu byť úmyselné alebo neúmyselné, pochádzať z vnútra organizácie alebo zvonku.

Dôsledky úniku údajov môžu byť vážne a dlhotrvajúce, vrátane poškodenia reputácie, finančných strát, prerušenia prevádzky, právnych následkov a strát duševného vlastníctva. Mnohé organizácie sa v súčasnosti zameriavajú na implementáciu najlepších postupov v oblasti kybernetickej bezpečnosti, aby predišli únikom údajov.[6]

Obr. 1 Dôvody výskytu bezpečnostného incidentu

* + 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.[7]

Graf č.1 Zdroj: Autorka práce

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.



Obrázok č.2 Dvojfaktorová autentifikácia. Zdroj: < https://www.antivirus-zadarmo.sk/dvojfaktorova-autentifikacia/ >

* 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.[8]

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. Produkt a jeho tvorba

Tvorba plagátu si vyžaduje zohľadnenie mnohých dôležitých faktorov, aby bolo možné efektívne sprostredkovať informácie cieľovému publiku. V mojom projekte som venovala pozornosť farbám, textu, cieľovému publiku, obsahu a použitiu ilustrácií na zvýšenie vizuálneho účinku.

* 1. Cieľová skupina

Cieľová skupina môjho plagátu o bezpečnosti na sociálnych sieťach zahŕňa mladšie aj staršie generácie.

1. Mladšie generácie, ktoré sú aktívne na sociálnych sieťach, si často neuvedomujú všetky riziká spojené s online aktivitami. Mnohí z nich nemusia byť dostatočne informovaní o bezpečnostných otázkach, ako je phishing, kyberšikana alebo únik osobných údajov. Preto je mojím cieľom pomôcť im rozpoznať tieto hrozby a naučiť ich, ako sa chrániť online.
2. Staršia generácia, hoci nie je taká aktívna na sociálnych sieťach, je stále vystavená nebezpečenstvám online sveta. Môžu sa stretnúť s phishingom, podvodmi alebo inými druhmi online trestnej činnosti. Je dôležité, aby pochopili, ako pri interakcii so sociálnymi médiami chrániť seba a svoje údaje.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **13-17** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65+** |
| Male | 2.7% | 12.6% | 17.6% | 10.9% | 6.1% | 3.5% | 2.6% |
| Female | 2.1% | 8.9% | 12.3% | 8.5% | 5.5% | 3.8% | 3% |

Tabuľka č.1 Distribution of Facebook users worldwide as of January 2024, by age and gender. Zdroj: Stacy Jo Dixon < https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/>

Môj plagát je teda navrhnutý s ohľadom na obe cieľové skupiny, aby bol zaujímavý a užitočný tak pre mladých používateľov sociálnych médií, ako aj pre starších ľudí, a pomohol im lepšie pochopiť riziká a naučiť sa, ako sa v online svete chrániť.

* 1. Farby

Použitie jasných farieb, ako je ružová, fialová a modrá má niekoľko dôležitých výhod.

1. Pritiahnutie pozornosti: Jasné farby, ako sú ružová, fialová a modrá, okamžite upútajú pozornosť čitateľov. Vystupujú z pozadia a ľahko priťahujú pohľady, vďaka čomu je plagát viditeľnejší a atraktívnejší.
2. Asociácie s bezpečnosťou: Niektoré farby, napríklad modrá, sa spájajú so spoľahlivosťou a bezpečnosťou. Použitie týchto farieb na plagáte môže zdôrazniť dôležitosť témy bezpečnosti v sociálnych médiách a posilniť myšlienku.
3. Emocionálny vplyv: Ružová a fialová farba môžu v čitateľoch vyvolať aj určité emócie, napríklad pohodlie a pokoj. To môže pomôcť vytvoriť pozitívny dojem z prezentovaných informácií o bezpečnosti v sociálnych médiách.
4. Estetická kombinácia: Ružová, fialová a modrá sú harmonické farby, ktoré môžu na plagáte vytvoriť príjemný a príťažlivý vizuálny dojem. Ich kombinácia dodáva plagátu estetickú príťažlivosť a robí ho zapamätateľnejším.

Výber ružovej, fialovej a modrej farby teda nielen priťahuje pozornosť čitateľa, ale aj zdôrazňuje dôležitosť témy, vytvára emocionálny dojem a poskytuje estetickú kombináciu na plagáte.

* 1. Text a jeho obsah

Pri výbere textu a jeho obsahu na plagáte sa zohľadnilo niekoľko dôležitých aspektov.

1. Jednoduchosť a zrozumiteľnosť: Text bol zvolený tak, aby bol čo najzrozumiteľnejší pre široké čitateľské publikum. Boli použité jednoduché a prístupné formulácie, aby sa predišlo prípadným ťažkostiam pri čítaní textu. To umožňuje, aby aj osoby bez špecializovaných znalostí o bezpečnosti na internete pochopili hlavné myšlienky uvedené na plagáte.
2. Zväčšený nadpis: Nadpis bol zväčšený, aby ešte viac upozornil na kľúčovú tému bezpečnosti sociálnych médií. To pomáha zvýrazniť hlavné myšlienku plagátu a vyniknúť medzi ostatnými prvkami dizajnu.
3. Stručný úvod do témy: Obsah textu bol obmedzený na stručný úvod do témy bezpečnosti sociálnych médií. Slúži to na to, aby čitateľov zaujal a aby sa chceli o tejto dôležitej téme dozvedieť viac.

Text a obsah plagátu bol teda starostlivo vybraný tak, aby boli informácie prístupné a príťažlivé pre široké spektrum používateľov, aby upozorňovali na kľúčovú tému a motivovali čitateľov k hľadaniu ďalších informácií o bezpečnosti na sociálnych sieťach.

* 1. Ilustrácie

Ilustrácie na plagáte boli vybrané tak, aby boli informatívne, jednoduché a v súlade s témou bezpečnosti sociálnych sietí. Bolo dôležité vybrať obrázky, ktoré by pomohli vizualizovať hlavné aspekty témy a upútali pozornosť čitateľa.

Jednoduchosť ilustrácií umožňuje rýchle pochopenie hlavných myšlienok prezentovaných na plagáte bez zbytočnej zložitosti alebo zmätku. To je dôležité najmä vzhľadom na to, že plagát musí byť zrozumiteľný pre široké publikum vrátane mladšej aj staršej generácie.

Takže v procese tvorby plagátu na tému sociálnych médií sa zohľadňovali všetky podstatné aspekty, od výberu farieb a ilustrácií až po dizajn textu. Snažila som sa, aby bol dizajn čo najefektívnejší a najatraktívnejší a aby upozornil na dôležitú tému bezpečnosti sociálnych médií.

1. Záver

Na záver by som rád zdôraznila dôležitosť bezpečnosti sociálnych sietí a dôležitosť správneho vzdelávania a informovanosti v tejto oblasti. S rastúcim využívaním sociálnych médií si musíme byť vedomí rizík spojených s online interakciami a vedieť, ako sa chrániť pred potenciálnymi hrozbami.

Je mimoriadne dôležité, aby sme sa ako používatelia sociálnych sietí naučili rozpoznávať znaky phishingu, kyberšikany a iných foriem online útokov. Zároveň by sme sa mali oboznámiť s možnosťami zabezpečenia účtu, ako je dvojfaktorová autentifikácia a používanie silných hesiel.

Okrem toho by sme mali venovať pozornosť aj tomu, aby sme pochopili, ako sú naše osobné údaje spracúvané a chránené na sociálnych sieťach. Súkromie a bezpečnosť údajov sú jadrom digitálnej bezpečnosti a dôvery v našom online prostredí.

Zoznam použitej literatúry

1. ESET, spol. s r.o. Malvér. [online]. [cit. 2024-04-05] Dostupné na internete: <https://www.eset.com/sk/malver/>
2. Barbora Netolická. Sociálne inžinierstvo v kontexte informačnej bezpečnosti v organizácii. [online] [cit. 2024-04-05] Dostupné na internete: <https://www.eset.com/sk/firemna-it-bezpecnost/bezpecnostne-sluzby/services/clanky/socialne-inzinierstvo-ib/>
3. David Harley & Andrew Lee. Phishing. [online]. [cit. 2024-04-05] Dostupné na internete: < https://web-assets.esetstatic.com/wls/2012/11/PhishPhodder.pdf/>
4. David&Harley. Online Shopping and a Phishing. [online]. [cit. 2024-05-01] Dostupné na internete: < https://web-assets.esetstatic.com/wls/200x/phish-pheeding-phrenzy.pdf >
5. UNICEF. Cyberbullying: What is it and how to stop it. [online] [cit. 2024-04-21] Dostupné na internete: <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>
6. Microsoft. Čo je únik údajov? [online]. [cit. 2024-04-05] Dostupné na internete: < https://www.microsoft.com/sk-sk/security/business/security-101/what-is-a-data-breach>
7. Скандал навколо Facebook: хто і навіщо злив дані 50 мільйонів користувачів. [online]. [cit. 2024-04-05] Dostupné na internete: < https://www.epravda.com.ua/publications/2018/03/20/635159/ >
8. PLEVA Matúš. Biometrické systémy bezpečnosti. Technická univerzita v Košiciach 2021. ISBN: 978-80-553-3834-7. Dostupné na internete: < https://www.kemt-old.fei.tuke.sk/KEGA009TUKE-4-2019/BSB-ucebnica.pdf >