Západočeská univerzita v Plzni

Bezpečnost informačních technologií

KIV/BIT

Dokumentace semestrální práce Bezpečnost sociálních sítí

Jakub Vaněk
A16B0160P
vanekjak@students.zcu.cz

15. května 2019

Obsah

1 Úvod

Tématem semestrální práce je bezpečnost sociálních sítí. V první části bude stručně popsán pojem sociální síť a jejich historický vývoj. V druhé části budou popsány typy útoků na sociální sítě a způsob obrany proti těmto útokům.

2 Vývoj sociálních sítí

Sociální sítě jsou internetové služby umožňující uživatelům sdílet veřejně či částečně veřejně osobní i neosobní informace mezi ostatními uživateli. Uživateli těchto sítí mohou být osoby, skupiny, politické strany, firmy nebo i spolky. Uživatelé informace sdílí pomocí svého profilu, který si mohou po registraci vytvořit. Pomocí sociálních sítí mohou uživatelé vykonávat různorodé činnosti. Těmito činostmi mohou být vzájemná komunikace, sdílení souborů, fotek, vytváření událostí, sdílení jakéhokoliv druhu informací.

První pseudosocílní sítí byl samotný internet, kde se lidé snažili mezi sebou komunikovat. V 70. letech 20. století byly posílány první emaily, čím se začala utvářet síť uživatelů - Sociální síť.

2.1 Bulletin Board System

Jednou z prvních sociálních sítí byl také Bulletin Board System. Jednalo se o soubor elektronických nástěnek, v klasickém dosovském grafickém rozhraní, kde si uživatelé mohli vyměňovat informace různého, samozřejmě textového, druhu. Problémem byla skutečnost, že v jednu chvíli mohl být přihlášen pouze jeden uživatel a komunikace tak byla velmi pomalá.

2.2 SixDegrees

První moderní sociální sítí postavená na konceptu web 2.0 (web, v němž pevný obsah nahrazen prostorem pro sdílení a společnou tvorbu obsahu) byla síť SixDegrees. Tato síť vznikla v roce 1997 a umožňovala uživatelům vytvářet okruhy přátel a poté v těchto okruzích komunikovat. Sociální síť měla přes milion uživatelů. Síť se však stala finančně neúnosnou a v roce 2001 byla odpojena. Svým konceptem předběhla dobu.

2.3 Friendster

Další sociální sítí byla služba Friendster vytvořená v roce 2002. Tvůrci o rok později dostali nabídku od společnosti Google na odkoupení Friendsteru za 30 milionů dolarů. Tvůrci však nabídku odmítli. Friendster byla sociální síť sloužící k seznamování "přátelů přátel". Během prvního čtvrtletí své existence překročila hranici 3 milionů uživatelů. V roce 2009 byla síť odkoupena společností MOL Global za 26,5 milionu dolarů a v současné době slouží ke sdružení hráčů počítačových her.

2.4 MySpace

V roce 2003 byla spuštěna oblíbená sociální síť Myspace. MySpace dovoloval, kromě klasických funkcí úpravu grafického rozhraní profilu, přidávání audio přehrávače a fotografií. MySpace se stal internetovým super-fenoménem. V roce 2006 překonal hranici 100 miliónů registrovaných uživatelů a dokonce, jako jediný web na světě, předstihnul Google v žebříčku nejnavštěvovanějších stránek USA. MySpace funguje dodnes, její obliba však již není taková jako mezi lety 2006-2008 a to hlavně díky vzestupu Facebooku.

2.5 Facebook

V roce 2004 byla vytvořena snad nejrozsáhlejší a nejúspěšnější sociální síť Facebook. Tuto síť vytvořil Mark Zuckerberg se svými spolužáky na Harvardské univerzitě. Původně měla sloužit jako ročenka studentů. Postupem času expandovala na ostatní unverizty a v roce 2006 se otevřela pro veřejnost. V současné době má Facebook 2,4 miliardy uživatelů.

2.6 Další

V dnešní době jsou sociální sítě fenoménem a existuje jich velké množství. Za zmínku stojí sociální sítě Twitter, Instagram, Snapchat, Tumblr, LinkedIn, WhatsApp, Google+, Pinterest, YouTube.

3 Typy útoků a jak se jim bránit

Sociální sítě využívají miliardy uživatelů. Účelem útoků na sociální sítě může být snaha vyřadit síť z provozu na určitou dobu, nebo permanentně. Dalším účelem může být snaha o krádež osobních údajů o uživatelích pro zisk informací o nich, nebo může mít útočník snahu se za oběť vydávat.

3.1 Denial of Service

Denial of Service (DoS) je útok, který se snaží vyřadit stránku z provozu, nebo znemožnit uživatelům se k ní připojit. Útok probíhá odesíláním velkého množství požadavků na server. Během zpracování těchto požadavků server nestíhá řešit požadavky uživatelů a uživatel tak není schopen síť používat. Jedním z největších takových útoků byl DDoS útok na sociální síť GitHub. Přenos 1,35 terabitů ze sekundu byl zaznamenán 28.února 2018 v 17:30. Takto velké množství dat zlomilo rekord velikosti přenosu během DDoS útoku. Podle sítě GitHub pocházel útok z více než 1000 autonomních systémů.

Tomuto typu útoku se nevyhly ani sítě Facebook a Twitter, na které byl proveden DDoS útok 7.sprna 2009. Zatímco Facebook byl pouze výrazně zpomalen, síť Twitter byla nedostupná několik hodin.

Takovému útoku je možné se bránit rozdělením sítě na několik serverů, které budou mít různou lokaci. Zároveň existuje spoustu hardware a software, které dokáží síť před takovými útoky bránit.

3.2 Social Engineering

Hlavním bezpečnostní trhlinou všech sociálních sítí jsou vlastní uživatelé. Techniky sociálního inženýrství využívají lidských chyb a manipulace a získávají tak informace přímo od uživatelů. Nyní shrňme nejznámější metody sociálního inženýrství.

3.2.1 Pretexting

Pretexting je metoda, která využívá dostupných nebo jednoduše zjistitelných informací k působení škod. Většina sítí ověřuje své uživatele nejrůznějšími otázkami, jakou jsou třeba rodné číslo, nebo jméno matky za svobodna. Tyto informace se dají snadno získat přímo od uživatele. Útočník si dopředu vytvoří scénář (pretext) podle kterého postupuje. Pretextingový podvod probíhá většinou přes telefon nebo při osobním setkání, například na ulici. Jeho cílem je nenápadné vylákání důležitých informací z oběti. Je proto založen

na vyvolání důvěry a tu útočník buduje pomocí příběhu, scénáře, který je z části založen na pravdivých informacích do kterého vtáhne svoji oběť a systematicky se z ní snaží získat další informace, které potřebuje. Tyto informace následně může využít k ukradení identity, nebo k získání jiných potřebných informací. Díky takto získaným informacím pak může útočník vystupovat pod jménem oběti.

Proti takovému útoku je obranou zdravý rozum. Důležité je neposkytovat nikomu žádné informace, které by mohli být následně zneužity tímto způsobem. Neposkytovat takové informace po telefonu ani osobně. Samotné sociální sítě by se proti takovým typům útoků měli bránit nevyžadováním podobných informací k získávání hesel apod. K ověřování hesel a přihlášení je v dnešní době výhodnější využívat ověření pomocí jednorázového kódu zaslaným formou sms, tak jak to dělá například sociální síť Instagram.

3.2.2 Phishing

Jedním z nejznámějších útoků na uživatele je tzv. phishing. Útočník získává citlivé informace nebo hesla od oběti pomocí podvodných e-mailových zpráv. Forma těchto zpráv se snaží napodobit originální formu zpráv, kterou mohou sociální sítě využívat. Paradoxem je, že žádná sociální síť ani služba neověřuje hesla pomocí zaslání hesla do emailu, ale spíše internetovým formulářem, ale stále se najdou lidé, kteří své heslo v dobré vůli přes e-mail poskytnou. Internetové formuláře však ale dnes nejsou výjimkou a v takových chvílích je důležité zkontrolovat pravost takových stránek před odesláním formuláře.

Nejznámějším Phishingovým útokem byl pravděpodobně útok na službu iCloud 31.srpna 2014, kterému podlehlo nespočet známých osobností a z jejich iCloudového účtu jim byly ukradeny soukromé a někdy choulostivé fotografie.

Obranou proti takovému útoku je stejně jako u pretextingu zdravý rozum. Zásadní je nikdy nezasílat své přihlašovací údaje emailem ani žádným jiným způsobem. Pro zapomenutá hesla, nebo pro jejich změnu existují na sociálních sítích formuláře, které jsou důvěryhodné. Důležité je kontrolovat pravost těchto formulářů, pokud přijdou e-mailem. V takovém případě se může jednat o phishing.

3.3 Prolomení

Jedním z méně častých útoku je útok prolomením. Prolomení znamená, že útočník (běžně pomocí nějakého software) zkouší kombinace znaků a čeká, dokud některá z kombinací nebude správné heslo. Během toho čeká na odpověď serveru, který mu dá vědět, když zadal správné heslo a uživatele přihlásí.

Dnes tento typ útoku není příliš rozšířený, kvůli tlaku na uživatele, aby používali silná hesla a také omezeným počtem zadání hesla pro přihlášení.

Nejjednodušší obrana proti tomuto útoku ze strany uživatele je používat silné heslo. Například pokud bude heslo pětimístné a sestavené ze 3 malých písmen a 2 čísel, existuje přibližně 60 tisíc různých kombinací a prolomení bude na 2GHz procesoru trvat 0.03 sekundy. Pokud bude však heslo 12ti místné a sestavené ze speciálních znaků, čísel, malých a velkých písmen, prolomení na stejném procesoru bude trvat přibližně 7.5 milionu let. Sociální sítě tak mohou uživatele nutit využívat tyto kombinace znaků a šance na prolomení takového hesla je poté mizivá.

3.4 Malware

Malware je škodlivý software, který je skrytě nainstalován do počítače. Jedním z velkých případů takového softwaru byl tzv. "Facebookový virus"šířený v roce 2017. Tento virus dopomáhal útočníkům nabourat se do facebookového účtu uživatele a automaticky se šířit do sítě napadaného. Zároveň mohl být využit k získání citlivých informací z počítače, jako byla bankovní data, hesla apod. Facebookový virus je většinou šířen falešnými zprávami se závadnými odkazy. Tyto zprávy jsou navrženy skutečně lstivě, takže snadno vzbudí přirozenou zvědavost lidí a přinutí je na odkaz kliknout. Jakmile byl odkaz otevřen, virus napadl systém a začal zde vyvíjet aktivitu. Tyto typy software se mohou také šířit uvnitř her na sociálních sítích nebo jako jiné soubory.

Obranou proti takovému útoku ze strany uživatele musí být ověřování takových odkazů před jejich otevřením. Bohužel sociální sítě nemohou takovému šíření úplně dobře bránit bez toho, aniž by ověřovali veškeré odkazy a soubory, které jsou přes jejich služby odesílány, s čímž by ale paradoxně souhlasilo málo uživatelů, protože by měli pocit, že jsou sledováni.

3.5 Nepozornost

Posledním zmíněným útokem bude útok na nepozorného uživatele. V takovém případě může útočník vytvořit například jednoduchou hru, která ale při svém spuštění bude vyžadovat přístup k citlivým údajům na účtě, poloze apod. Uživatel často nevěnuje pozornost tomu, co vše aplikacím na sociálních sítích povoluje a může nevědomky poskytnout údaje, které nechce.

Jediná obrana proti takovému útoku je neposkytovat informace o účtu aplikacím a řádně si přečíst, co uživatel instalací a spuštěním povoluje.

4 Závěr

Největším nebezpečím sociálních sítí se zdá být lidská nepozornost a neinformovanost. V dnešním světě využívají sociální sítě všechny generace, včetně dětí, které jsou na tyto typy útoku nejnáchylnější. V takových případech je důležitá kontrola rodičů, protože je tak možnost předejít tragédiím, kdy se dítě vydá za útočníkem pod záminkou, že je to známá osoba. Sociální sítě jsou užitečné v mnoha ohledech avšak na to, jaké množství lidí tyto služby využívá, extrémně málo lidí o těchto útocích ví a dokážou jim předcházet.