

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky



Bakalářská práce

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Phishing v herním průmyslu

Vypracoval: Nguyen Van Thanh

Vedoucí práce: Ing. Ladislav Luc

Rok vypracování: 2016

Čestné prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Veškeré použité podklady, ze kterých jsem čerpal informace, jsou uvedeny v seznamu použité literatury a citovány v textu podle normy ČSN ISO 690.

V..... dne

Podpis:

.....

Poděkování:

Tímto bych chtěl poděkovat panu Ing. Ladislavu Lucovi za cenné rady a připomínky při zpracování této bakalářské práce.

Abstrakt

Tato bakalářská práce se zabývá v současné době závažnou problematikou zabezpečení kyberprostoru, kterou je phishing. Práce je specifická tím, že je zaměřena na oblast herního průmyslu, který je podroben detailní analýze.

Prvním cílem této práce je seznámit čtenáře s problematikou bezpečnostních rizik phishingu obecně a v herní oblasti. Pro dosažení tohoto cíle je v úvodu teoretické části práce představena obecná problematika phishingu z hlediska historického vývoje a rozšíření. Poté je podrobněji popsáno téma herního průmyslu s trendy videoher a s bezpečnostními riziky online obchodování.

Druhým cílem práce je poskytnout budoucím a stávajícím uživatelům platformy Steam přehled o běžných phishingových útocích a protiopatřeních. Pro dosažení druhého cíle je v analytické části práce vybrána konkrétní herní platforma v online obchodování a distribuci her, Steam od Valve, ke které jsou v praktické části práce vybrány osm phishingových útoků. K jednotlivým útokům je provedena stručná analýza, která je zakončena souhrnným vyhodnocením nebezpečnosti a protiopatření všech útoků.

Klíčová slova

phishing, scam, herní průmysl, videohra, STEAM

Abstract

This bachelor thesis deals with a currently major issue of cyber security, which is phishing. The study is also specific in that it is focused on the gaming industry, which is subjected to a detailed analysis.

The first goal of thesis is to acquaint the reader with problems of security risks of phishing in general and in game related fields. To achieve this goal, in the introduction of the theoretical part of the work, the general problem of phishing with a view on historical development and expansion is presented. Furthermore is described topic of gaming industry, its trends of videogames and security risks of online trading.

The second goal is to give future and existing Steam users an overview of common phishing attacks and countermeasures. To achieve this goal, in the analytical part of the work, a specific gaming platform in online trading and distribution of game is selected, Steam from Valve. In the practical part of the work, eight selected phishing attacks are conducted to brief analysis and completed into a final evaluation and countermeasures of all attacks.

Keywords

phishing, scam, game industry, video game, STEAM

OBSAH

1 Úvod	1
1.1 Volba tématu	1
1.2 Metodika řešení problematiky	1
1.3 Cíl práce	2
2 Phishing	3
2.1 Kyberkriminalita	3
2.2 Definice pojmu a vznik	3
2.2.1 Phishing.....	3
2.2.2 Pharming.....	4
2.2.3 První velké útoky	5
2.3 Výskyt a dopady v běžném životě	6
2.4 Útočníci	7
2.5 Anti-phishing Act.....	7
2.6 Další rozšíření	8
3 Herní průmysl	10
3.1 Úvod a hospodářství.....	10
3.1.1 Zábavní průmysl.....	10
3.1.2 Ekonomika	11
3.2 Historie a současnost.....	12
3.3 Videohra	14
3.3.1 Herní žánry.....	15
3.4 Herní platformy a vybavení	18
3.4.1 Struktura vývoje her	18
3.5 Trh herního průmyslu.....	19
3.6 E-sports.....	19
3.7 Sponzoři a partneři	22
4 Phishing a Scamming ve videohrách	23
4.1 Kultura her	23
4.2 Podvody.....	23
4.3 Černý trh.....	24
4.3.1 Komunita	24
4.3.2 Prodej a zneužití.....	24
4.4 Porovnání odlišností s běžným phishingem.....	25
5 Druhy útoků phishingu	26

5.1	Man-in-the-Middle.....	26
5.2	Falešná identita.....	27
5.3	Přesměrování.....	27
5.4	Vyskakovací okna	27
6	Možnosti ochrany	29
6.1	Antiviry	29
6.2	Anti-phishingové softwary.....	30
6.3	Blacklist.....	30
6.4	Dvoufaktorová autentizace	31
6.5	Shrnutí	31
7	Analýza herní platformy STEAM.....	32
7.1	STEAM	32
7.1.1	Úvod	32
7.1.2	Platforma.....	32
7.1.3	Steam obchod a chat	34
7.2	Působíště na trhu	34
7.2.1	Celosvětové zastoupení	35
7.2.2	Americký a český trh	37
7.3	SWOT analýza	38
8	Útoky na Steamu.....	39
8.1	Vybrané útoky	39
8.2	Kritéria vyhodnocení nebezpečnosti útoků.....	39
8.3	Metodika vyhodnocení útoku.....	42
8.4	Vyhodnocení všech útoků	43
8.5	Shrnutí	43
8.5.1	Cíl útoků	44
8.5.2	Zjištění informací oběti	44
8.5.3	Návnada	44
8.5.4	Rozeslání útoku	45
8.5.5	Zneužití získaných informací	45
8.5.6	Zahlázení stop	45
9	Zabezpečení na Steamu.....	46
9.1	Obecné návyky	46
9.2	E-mailové zabezpečení.....	47
9.3	SMS zabezpečení	47
9.4	SteamGuard	48
9.5	Závěrečné bezpečnostní vyhodnocení k vybraným útokům.....	49

10 Závěr	50
11 Terminologický slovník.....	52
12 Seznam použité literatury	54
13 Seznam obrázků a tabulek.....	62
14 Přílohy.....	63
14.1 Příloha 1: Phishing odkazy při obchodování	63
14.2 Příloha 2: Rychlé prohazování při obchodu.....	64
14.3 Příloha 3: Programy ke zlepšení hry	65
14.4 Příloha 4: Phishingový e-mail od společnosti.....	66
14.5 Příloha 5: SSFN kód.....	67
14.6 Příloha 6: Zneužití jména middlemana	68
14.7 Příloha 7: Paypal chargeback.....	69
14.8 Příloha 8: In-game scam	70

1 ÚVOD

1.1 *Volba tématu*

Téma bakalářské práce jsem si vybral ze dvou důvodů. Prvním důvodem je herní průmysl, neboť v herní oblasti se již několik let pohybuji a mohu čtenářům tuto oblast přiblížit. Herní průmysl je v dnešní době jedna z nejrychleji se vyvíjejících oblastí nejen z technologického hlediska, ale především jako cíl investorů. Mnoho peněz je zde obhospodařeno, a proto není divu, že jsou jednotlivci či celé organizace připraveny získat peníze z nic netušících uživatelů. Tím jsem naznačil druhý důvod zájmu o téma, kterým je bezpečnost uživatelů. Vybral jsem si konkrétní herní společnost, která je jedničkou na trhu v poskytování prodeje svých digitálních her a také je poskytovatelem her jiným vývojářům, denně s miliony uživateli online, Steam od Valve Corporation.

1.2 *Metodika řešení problematiky*

Bakalářská práce je členěna do tří částí, teoretické, analytické s analýzou konkrétní platformy a praktické s vyhodnocením vybraných útoků na herní platformě. Na začátku teoretické části popíši problematiku phishingu s obecným vysvětlením. Hlavním zdrojem informací, z něhož jsem čerpal, je kniha *Phishing exposed* neboli *Phishing bez záhad* od jedné z nejvýznamnějších osobností této oblasti James Lance. [1 str. 17] Autor publikoval mnoho knih s obdobnou tematikou.

Tématem práce je phishing v herním průmyslu, ke kterému v následujících kapitolách podrobně vysvětlím herní průmysl, online krádeže ve videohrách, jeho výskyt v životě a dopady. V závěrečných kapitolách teoretické části práce rozeberu útoky a ochranu proti phishingu. Zdroje jsou získány z odborných článků na portálu knihovny VŠE¹ a dalších elektronických zdrojů.

Následuje druhá část práce, ve které představím a analyzuji Steam platformu a její tržní situaci. V praktické části práce analyzuji útoky a podvody pomocí phishingu v různých formách na platformě a hrách Steamu, ke každému útoku uvedu vyhodnocení a opatření. Práce je zakončena kapitolou, v níž jsou uvedena všeobecná doporučení správného zabezpečení na Steamu.

¹ Vysoká škola ekonomická v Praze.

1.3 Cíl práce

Bakalářská práce má dva cíle. Prvním cílem práce je přínos získaných informací k pochopení postupů krádeží při online obchodování ve formě phishingu, a to obecně a v herní oblasti. Druhým cílem práce je poskytnout budoucím a stávajícím uživatelům platformy Steam přehled o běžných phishingových útocích a protiopatřeních, který může sloužit jako dílčí návod zabezpečení v jiných herních a i mimo herních platformách.

2 PHISHING

V této kapitole je přiblíženo téma dnešní moderní elektronické kriminality; zvané také kyberkriminalita. Poté se práce zaměří na jediný druh online krádeže, phishing, s podrobným vysvětlením a názornými ukázkami této problematiky. Kapitola je členěna do těchto částí:

- Kyberkriminalita;
- Definice pojmu a vznik (Phishing, Pharming a první velké útoky);
- Výskyt a dopady v běžném životě;
- Útočníci;
- Anti-phishing Act;
- Další rozšíření.

2.1 *Kyberkriminalita*

Počítačová kyberkriminalita je nehmotná krádež peněz a dalších citlivých informací institucí a samotných lidí realizovaná prostřednictvím počítače. Patří sem i tradiční forma kriminality, u které byl počítač či počítačové sítě použity s cílem usnadnění zločinu. [2]

Jde o téma, které je v současné době velmi diskutováno, neboť se mu nelze zcela vyhnout. Cíl útočníků je vždy stejný, a to krádež identity, sabotáž, vydírání a další trestné činy. I když společnosti předpovídají útoky či hrozby a náležitě se zabezpečí novými prostředky, útočníky to nezastaví. Útoky zpočátku pominou, ale v průběhu času se útočníci přizpůsobí a obejdou bezpečnostní překážky, proto je vždy potřeba průběžně aktualizovat své bezpečnostní složky.² [3] [4]

2.2 *Definice pojmu a vznik*

2.2.1 Phishing

Phishing je způsob okrádání uživatelů na internetu pomocí zfalšovaných stránek s cílem zjistit a zneužít jejich osobní údaje. Pojem phishing je z anglického slova fishing neboli rybaření, kdy si lze útočníka představit jako rybáře, který pomocí háčků, v tomto případě falešné webové stránky, chytá své ryby neboli oběti - phishe. [1] Phishing je součástí scamu³, který představuje obecně veškerý druh online krádeží za pomoci falešné identity.

² Antiviry, firewally, školení zaměstnanců a další.

³ Scam je podvodné jednání při obchodování.

Cílem phishingu je zneužití získaných údajů za pomoci falešných stránek, na které oběť klikne.⁴

Nejdůležitějším nástrojem phishe jsou webové stránky, které fungují na principu oklamání oběti webovým designem, který je vždy totožný s původní stránkou. Útočník se v této situaci prezentuje jako konkrétní společnost. Po navštívení stránky jsou oběti vyzvány zkontrolovat si přihlašovací údaje nebo jsou v jiných případech nuceny přihlásit se na stránku. Poté, co jsou vyplněny údaje a oběti přesměrovány někdy i na pravou webovou stránku [5], se útočník k těmto údajům dostane. Využil metodu přesměrování, která bude níže podrobněji vysvětlena v kapitole 5.3, způsobem MITM⁵.

Další součástí phishingu je prostředek šíření phishe. K tomu se využívají nejčastěji e-maily či zprávy sociálních sítí. Výhodou je, že útočník bez jakýchkoliv zábran může navázat kontakt s jakoukoliv vyhlédnutou obětí. Obsah zprávy je ne zcela jednoduše rozpoznán, a to ani odborníky. Jediným způsobem bezpečné a ověřené komunikace je takzvaná metoda end-to-end, která využívá digitálních podpisů, například PGP nebo S/MIME.⁶ [1 str. 19]

V některých případech se v odkazu, který je odeslán útočníkem, vyskytuje malware. Malware je škodlivý software vytvořený útočníkem s konkrétním účelem. Cílem těchto programů je krádež, modifikace či zničení dat z počítače. Mezi malware patří počítačové viry a červi, dále trojské koně, spyware a adwary. [6] Viz kapitola 2.6.

2.2.2 Pharming

Sofistikovanější a nebezpečnější druh phishingu je pharming. Pharming lze označit jako nástupce phishingu, který se zaměřuje zejména na obměnu IP adresy v systému pomocí malwaru, tedy útoku na DNS⁷. Oběť podvodu je přesměrována na falešnou webovou stránku, i když správně zadala název vyhledané IP adresy, a dále funguje princip výše popsaného phishingu.

Koloběh spear phishingu

V této části je názorně popsán koloběh útoku. Oproti běžnému phishingu lze považovat spear phishing za cílený phishing na konkrétní organizaci, avšak funguje na stejném principu, viz Obrázek 1.

⁴ Oproti tomu v hacku se útočník snaží proniknout bez vědomí uživatele a tímto získat jejich data.

⁵ MITM – Man-in-the-Middle.

⁶ Programy umožňující šifrovanou komunikaci mezi odesílatelem a koncovým příjemcem.

⁷ DNS – Domain name server je počítačově pojmenované jakékoliv zařízení či služba připojená k internetu. [80]



Obrázek 1 Koloběh spear phishingu [7], přeložil: Autor

Clone phishing

Ke spear phishingu lze přiřadit také clone phishing, který se však zaměřuje na konkrétní osobu. Útok spočívá v získání informací internetového chování oběti, tj. historie, nejnavštěvovanější stránky, fóra, všechny zmíněné položky vyžadují přihlášení, na kterém bude útočník zakládat svůj phish. [8]

2.2.3 První velké útoky

Začátek byl spojený s America Online⁸, když se v roce 1995 vyskytl první phish, automatizované procesy phishingu zaměřené na údaje účtů a kreditních karet. Oběti byly vyzvány, aby si aktualizovaly přihlašovací údaje, a to z důvodu technických potíží při transakci. Útoky byly provedeny s pomocí zpráv od falešného administrátora společnosti, phishera. Tehdy měla tato metoda veliký dopad, neboť osobní počítač a internet byly novinkou. Nezasahovaly tak širokou část populace jako v dnešní době. [1]

V roce 2003 se phishing poprvé zaměřil na finanční instituce, terčem byly veškeré jejich bezhotovostní peníze. Oproti prvnímu phishi s sebou přinesl několik vylepšených forem

⁸ America Online (AOL) je mezinárodní poskytovatel internetových služeb a první významnou obětí phishingu.

útoků, proti kterým se nešlo bránit pomocí zabezpečení IT a zabudování antivirů, neboť phishingové útoky využívaly lidský faktor, zejména nevědomost a nezkušenost. Byly zaznamenány další velké úspěchy phishingu a s nástupem útoků vyskakovacích oken se phishing dále rozvíjel. I když princip útoků je stále stejný a již známý, funguje dodnes ještě sofistikovanějšími metodami. [9]

2.3 Výskyt a dopady v běžném životě

Pojem phishing se vyskytuje ve všech oblastech obchodování a jiných peněžních transakcích, ve virtuální a reálné formě na základě celosvětových online fór www.ScamVictimsUnited.com [10] a www.ScamSurvivors.com [11] a jednoho českého www.ViRy.Cz [12], která se zabývají obětmi nejrůznějších druhů phishingu.

Mezi nejčastějšími cíli online podvodů byly finanční instituce, šlo zejména o banky. Obětem těchto podvodů bylo zasláno upozornění na nové aktualizace prostřednictvím e-mailu či jiné upomínky. Přestože je tento způsob okrádání jedním z nejtypičtějších v minulosti i současnosti, stále je úspěšný. K dalším tématům patřily e-maily s předmětem eBay, Amazon a dalších online obchodů, v nichž byla oběť nucena aktualizovat své bankovní údaje. Falešné finanční poradenské služby a obdobné služby také nebyly výjimkou.

Sociální sítě nebo internetové seznamky jsou v dnešní době hojně zneužívány, převážně pak Facebook, který má širokou oblast působení. V těchto případech se útočník snaží nalákat na klamavé reklamy, získat tak přístup na facebookový účet oběti. U internetových sezonek je útok nejčastěji uskutečněný za pomoci falešné identity a prostřednictvím konverzace dojde k dosažení cíle útočníka.

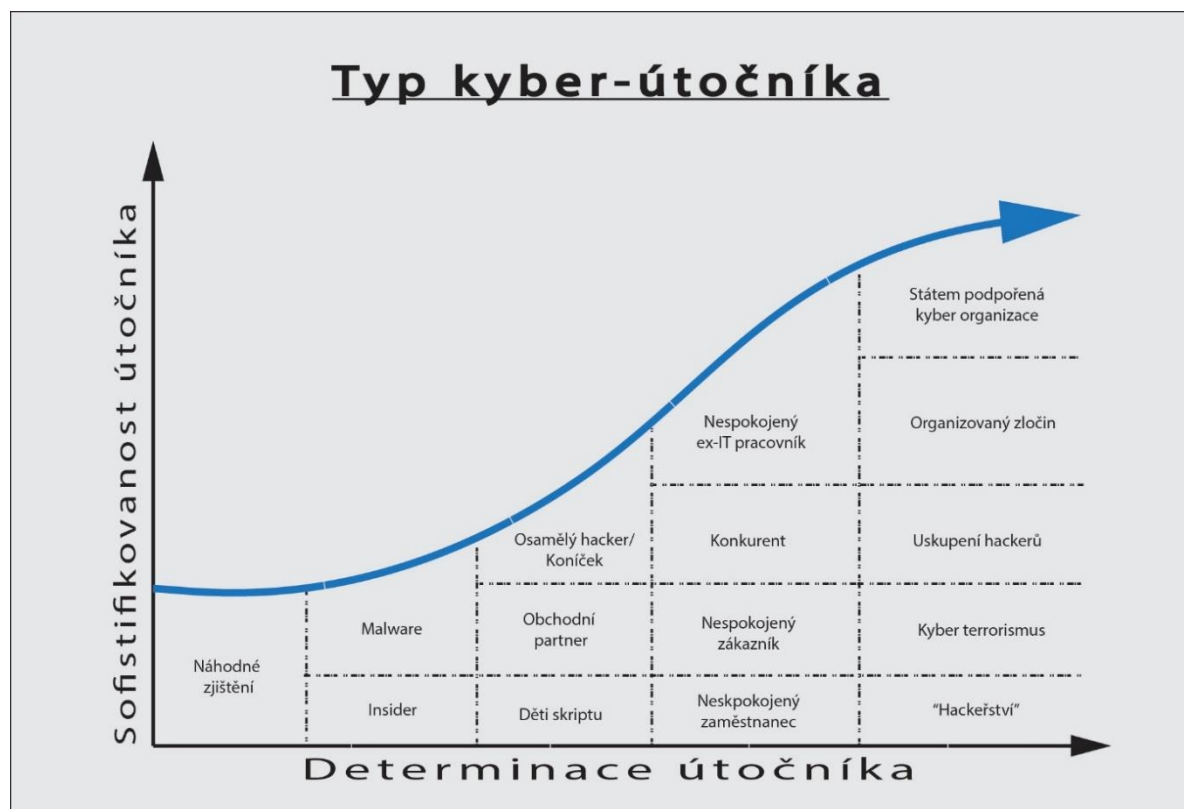
K zajímavým tématům patřily například přírodní katastrofy a charitativní akce, kdy zloděj využil lidskou laskavost a nabádal k přispění obětí penězi.

Nejenže se podvodné zprávy šíří počítačem, ale v dnešní době existují další formy krádeží, jako jsou podvodné SMS zprávy a telefonáty.

2.4 Útočníci

Kvalifikace útočníků

Online útočníkem se může stát kdokoliv, rozdíl je však v jeho schopnostech ovládat jednotlivé útoky a rozumět jejich principům. Existuje několik motivů, proč útočit. Peníze a poškození reputace organizace jsou nejčastějším motivem. Na obrázku (Obrázek 2) je podrobněji vysvětlena současná situace útočníků a také jejich členění.



Obrázek 2 Typ kyberútočníka [75], přeložil: Autor

Nejzajímavější informací (viz Obrázek 2) je to, že jednou z nejčastějších příčin útoků je nespokojenost až nenávist jedince ke konkrétní společnosti či instituci a snaha poškodit například její reputaci v dalším podnikání. Tyto osoby nemusí být vždy schopny útoku, avšak dokáží si nelegálně objednat službu hackerů. Ti spíše (jako odborníci) realizují útok a dokončí ho jako skupina či organizace. Jednotlivci nemají dostatek motivace/determinace k útoku, neboť lze během něj očekávat komplikace, naopak ve skupině lze cíle dosáhnout rychleji a efektivněji.

2.5 Anti-phishing Act

Phishing je trestná činnost, a proto vznikly zákony související s touto problematikou, která byla řešena zejména ve Spojených státech. Mezi první zákony proti phishingu lze

řadit Anti-phishing Act z roku 2004, 2005 a 2008, následují Anti-phishing Warning a zlaté pravidlo, které zní „*Nikdy neklikejte na horkou linku v textu e-mailu*“. [13]

Nyní je stručně popsán obsah současného znění Anti-phishing Act od společnosti ALEC⁹. [13]

Zákon je dělený do deseti sekcí se stručným shrnutím problematiky phishingu a pharmingu na začátku. První sekce popisuje všechny položky zákona, kterými jsou společnosti, jedinci, identifikované informace, falešné údaje a webová stránka. Ve druhé sekci je stručně vysvětlena situace, za jakých okolností se někdo stane vinným z phishingu a pharmingu. Ve třetí sekci se řeší imunita phisherů, v případě poskytovatel webového serveru či internetu zruší své služby, na kterých běžely phishingové stránky. Tito poskytovatelé nejsou stíháni a nuceni uvést důvod. Čtvrtá sekce řeší prohřešky a následky phishingu a pharmingu, v páté sekci se popisují možnosti hlášení podvodů a v následujících sekcích se řeší administrativní tohoto zákona, jako je odvolatelnost, zrušení a funkčnost zákona od konkrétního data.

2.6 Další rozšíření

Phishing s sebou nese také další nebezpečí. Kromě ztráty údajů a dat může být nakažen a modifikován počítač oběti. Níže jsou stručně popsány druhy nejčastějších malwareů použitých při phishingu.

Počítačový vir a červ

Počítačové viry a červi jsou speciální programy, které slouží k narušení či likvidaci konkrétní služby na počítačové síti a v systému uživatele. [14] Virus je oproti červu, který se šíří pomocí síťových paketů, obsažen v elektronických poštách, šíří se prostřednictvím infikovaných souborů při spuštění určitých programů s příponou.exe (executable). [15]

Trojské koně

Na rozdíl od virů a červů jsou trojské koně méně nebezpečné, neboť nemají schopnost replikace, a proto neinfikují další soubory. Trojské koně nepřicházejí s infikovanými soubory, ale je zapotřebí spustit samotného trojského koně. Ten se k uživateli chová jako užitečný spustitelný program. [15]

Spyware a adware

Oba tyto programy jsou druhem cílené reklamy. U spywaru jsou uživatelům ukradena data o jejich internetových aktivitách, tím je vytvořena určitá reklama.

⁹ ALEC - American Legislative Exchange Council.

U adwarů jsou typická „vyskakovací“ okna a reklamy na internetových stránkách či programech. Tyto programy většinou nenesou škodlivé následky, ale jen uživateli „překáží“. Adware slouží také jako placená reklamy u takzvaných „free“ programů¹⁰, u nichž lze tyto reklamy vypnout za příplatek.

¹⁰ Většinou se jedná o demo verze aplikací.

3 HERNÍ PRŮMYSL

Pro pochopení této práce je zapotřebí čtenáři částečně přiblížit téma herního průmyslu. V této kapitole se podrobněji rozeberou základní údaje a vlastnosti herního průmyslu. Kapitola je členěna následovně:

- Úvod a hospodářství (Zábavní průmysl, Ekonomika);
- Historie a současnost;
- Videohra (Herní žánry);
- Herní platformy a vybavení;
- Trh herního průmyslu;
- E-sports;
- Sponzoři a partneři.

3.1 Úvod a hospodářství

Posledních 40 let herní průmysl výrazně vzrostl, dostal se do povědomí společnosti bez ohledu na věk a pohlaví. Postupem času se rozšířily možnosti dostupnosti hraní na počítačích, mobilních zařízeních, tabletech, přenosných konzolách a dalších. Ačkoliv se průmysl vyvinul do dnešní podoby, musí si vždy držet krok s novými technologiemi, po nichž poptávka spotřebitelů roste. [16]

3.1.1 Zábavní průmysl

Herní průmysl je v současnosti jedním z nejvýznamnějších ekonomických sektorů v oblasti zábavního průmyslu, mezi něž patří hudební a filmový. I když je součástí těchto „starých“ průmyslů, je odlišný ve své komplexnosti. K základním aktérům tohoto odvětví patří autoři a vydavatelé. Ale u herního průmyslu se místo označení autoři používá herní vývojáři, vedle nichž nelze opomenout další spoluúčastníky jedinečné svými schopnostmi. Patří sem například herní designéři, architekti, návrháři, dále poskytovatelé herních platform, softwarů, hardwarů a serverů, důležitou roli hrají také zákazníci, kteří mnohdy nasměrují vývoj her k její finální podobě. [17]

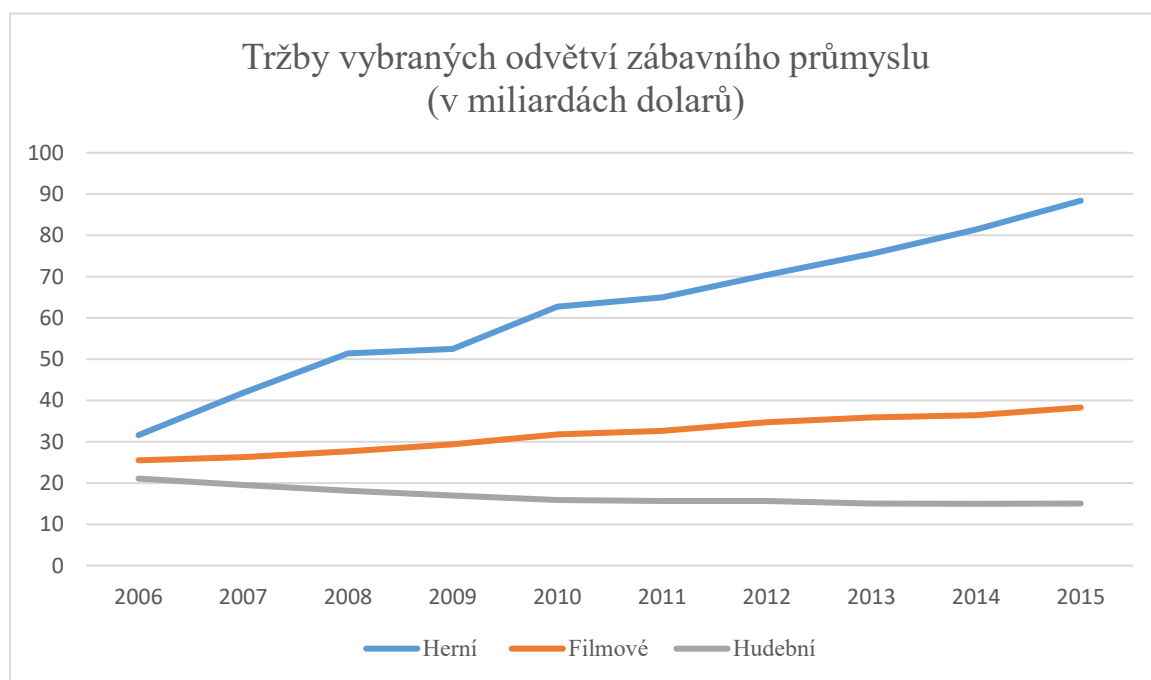
Existují další rozdíly, a to zejména v hospodářství a jejich způsobu podnikání. Například ve filmovém průmyslu je zisk z prodeje licencí do televizního vysílání, z prodeje DVD a z pronájmů filmů. U hudebního průmyslu je situace obdobná jako u filmového průmyslu, zisk přináší z velké části prodej licencí do filmů a rádiových vysílání. K sekundárním tržbám hudebního průmyslu patří i samotná účast zpěváků, kteří v současné době jezdí na turné, hrají svou hudbu živě. Avšak hlavním zdrojem a také odlišností herního průmyslu

je přímý prodej spotřebitelům. Zisk je přijímán formou digitální či fyzické koupě videohry, měsíčního placeného odebrání nebo nepřímými způsoby, kliky na webový server her. Do sekundárních příjmů je zahrnut i prodej licencí jako u výše zmíněných odvětvích zábavního průmyslu. [18 str. 16] Ale jelikož hry nefungují bez určitých komponentů, jako jsou počítač, herní konzole, myš, herní joystick, mobilní telefon, internet a další periferie, nelze jednoznačně určit celkovou výši investic do her a herního průmyslu.

3.1.2 Ekonomika

Dle celosvětových statistik se v roce 2013 v herním průmyslu vydělalo dvakrát více než ve filmovém. Trend her nepřestává růst, podle serveru NewZoo se očekává překročení hranice 100 mld. dolarů vydělaných herním průmyslem v roce 2017, a to díky vzrůstu poptávky po mobilních hrách v nadcházejících letech v Číně. [19] [20]

Níže je zpracovaný graf (**Error! Reference source not found.**) historického vývoje vybraných sektorů v zábavním průmyslu. Herní průmysl oproti jiným jako jediný výrazně roste, ale musí se brát v potaz, že v hudebním a filmovém průmyslu jsou zahrnuty jen přímé prodeje desek či filmů digitálně a fyzicky ze serveru MPAA¹¹ [19]. V grafu lze vidět, že hudební průmysl má klesající trend a v současné době celosvětově stagnuje na hodnotě 15 mld. dolarů. Nepatrně lepší situace je ve filmovém průmyslu, který má tendenci mírného růstu díky novým 3D technologiím a virtuální realitě.



Obrázek 3 Vývojové trendy v zábavním průmyslu [4] [22] [23] [19] [24] [25] [20], zpracoval: Autor

¹¹ MPAA - Motion Picture Association of America.

Součástí herního průmyslu je také online streaming, který v posledních letech výrazně vzrostl. Mezi hlavní představitele patří mezinárodní platforma Twitch.tv, která byla v roce 2014 zakoupena za 970 mil. dolarů Amazonem. [21]

3.2 *Historie a současnost*

Herní průmysl představoval v minulém století něco nového a velmi složitého, proto není divu, že prvními zeměmi zabývajícími touto tematikou byly Spojené státy, Velká Británie a Japonsko. Ostatní země se až nástupem moderní doby podílí na tomto průmyslu. V následující podkapitole jsou stručně popsány klíčové momenty jeho vývoje.

20. století

První zmínky o videohrách se datují od 50. let, kdy počítačový nadšenec A. S. Douglas, student Cambridgeské univerzity, naprogramoval hru zvanou OXO nebo Noughts and Crosses¹² na počítači EDSAC pro svoji disertační práci. Hra nebyla nijak úspěšná, protože zařízení EDSAC bylo obrovské ve srovnání s dnešními počítači. Důvodem bylo i to, že počítač vlastnila pouze Cambridžská univerzita. [26] Druhou datovanou videohrou je Tennis for Two (Tenis pro dva) od W. Higginbothama, který oproti statické hře OXO dokázal jako první rozpohybovat na počítači grafiku objektu. Předurčil také další komponenty současných herních konzolí, jako je počítač zapojený do obrazovky a ruční analog. Ale stejně jako hra OXO neměla velké úspěchy z důvodu drahých součástí pro sestavení.

13

Na začátku 60. let byla na školním počítači Michiganské univerzity MIT vyvinuta hra Spacewar od Stevena Russella. Ohlas měla zejména mezi vysokoškolskými studenty, kteří se adaptovali na programovací jazyk hry a zkoušeli sami vyvíjet. Tím nastartovali první éru herního průmyslu. [27 str. 36]

Roku 1972 byla vyvinuta první herní konzole Odyssey, která dokázala měnit hry pomocí vyměnitelných kazet. Téhož roku Nolan Bushnell, jeden z nadšenců Spacewar, založil společnost Atari s hrou Pong, která byla vylepšenou verzí Tennis for Two od Higginbothama a fungovala na principu herní arkády, mince za hru. [28] V následujících letech se z Atari stala Atari VCS, která poskytovala na svém herním systému vývoj her. Společnost zůstala sedm let dominantní na trhu, ale poté tržby padaly kvůli špatnému vedení, marketingu a zpracování her. [29] Nakonec společnost zkrachovala, což zapříčinilo i dočasné zastavení celého průmyslu. V 80. letech situaci využila japonská společnost Nintendo,

¹² Obdoba piškvorek.

¹³ Podle syna spoluautora, Dvorak JR., by se vyčísnila na 20 000 dolarů dnešních hodnot. [72]

která vsadila na nový způsob a technologie hraní, a to na domácí systémy/konzole Nintendo Entertainment Systém (NES). [30] Úspěchy byly ohromné, herní trh byl těmito konzolemi zaplaven zejména v Japonsku. V následujících letech přišly na trh první přenosné herní konzole GameBoy, Nintendo si tak zajistilo první příčku v herním průmyslu na příštích 10 let. Hernímu trhu také konkurovaly další společnosti¹⁴, ale neprosadily se jako Nintendo. Změna nastala až v moderní době (tj. rokem 2000), nástupem dostupného internetu a chytrých mobilů. [29]

Nástup 21. století

S ústupem Nintendo na trhu, které se zaměřilo na vylepšení GameBoy, přišly na scénu další herní společnosti. Konzole od Sony generace Playstation (PS1 a PS2) a od Microsoftu XBOX (Xbox a Xbox 360) se počátkem moderní doby staly špičkou na trhu. [31] Na konci tisíciletí se internet dostal i do herních konzolí, a i když už dřívější produkty byly se zabudovaným internetovým přístupem, ohlas byl až s nástupem nových generací konzolí Playstation 3 s Playstation Network [32] a Xbox Live na Xbox 360. [33] Mezníkem je také nástup 3D her z původních 2D her. [34]

Je však nutné připomenout, že vzestupem užití internetu se na scénu dostávají i tradiční osobní počítače. Vznikl nový žánr online her s tisíci lidí online, MMORPG¹⁵, který se stal jedním z nejhranějších žánrů her. Nejprodávanější počítačovou hrou roku 2006 se stala hra World of Warcraft od Blizzardu [31], která je stále vyvíjena a hrána dosud s více než 10 milióny měsíčních předplacení. [35] S tímto žánrem se pojí i externí služby, například Voice-over-Internet Protocol (VoIP), které zprostředkovávají hlasovou komunikaci mezi hráči [36], neboť některé hry nemají dostatečnou kvalitu pro hráče či neumožňují tuto funkci. [37]

Další oblastí, která byla na vzestupu, je oblast sociálních sítí, jejímž hlavním iniciátorem se stala síť Facebook založená v roce 2004. [29] Facebook byla zpočátku jen univerzitní sociální síť vytvořená studenty Harvardské univerzity v čele s M. Zurckerbergem. Avšak po dvou letech se Facebook rozšířil celosvětově [38] a umožnil herním vývojářům a dalším prosadit se v této platformě a prodávat své produkty. Mezi prvními hity sociálních sítí byly nenáročné hry jako Texas HoldEm' Poker¹⁶ a Scrabulous¹⁷. [39] Facebook také poskytl službu, kterou doposud nikdo nedokázal. Každý uživatel měl možnost pozvat své kamará-

¹⁴ Microsoft Corporation a Sony Entertainment.

¹⁵ MMORPG Massively Multiplayer Online Role Playing

¹⁶ Online hra na způsob pokeru.

¹⁷ Česká obdoba křížovek.

dy přímo prostřednictvím Facebooku, tedy všichni byli potenciálními herními přáteli a překážky k hraní byly téměř nulové.

Současná situace

Poslední roky se vývoj her soustřeďuje na takzvané „casual“ hráče, oproti „hardcore“ hráčům jsou jejich požadavky na grafiku zpracování daleko nižší, nezávislé na grafické náročnost hry. „Casual“ hráči nejsou povinni a ani nechtějí vynaložit tolik času na danou hru. [40] Takovou metodou funguje dnešní mobilní trh, který je nejrychleji rostoucí ze všech herních segmentů. [41] Smartphony v dnešní době vlastní téměř každý a při připojení na internet si mohou zájemci stáhnout jakékoliv programy a hry prostřednictvím AppStore od Applu, Google Play od Googlu a další.

Trendem současné doby je, že se hry postupem času ukládají na cloudových serverech, aby ulehčily rendering¹⁸ grafiky na počítači nebo jiné konzoli. [39] Důvodem je snaha snížit zatížení počítače z hardwarového hlediska a také zvýšit bezpečnost tím, že jsou údaje ukládány na daném serveru hry.

Posledním hitem jsou nově vzniklé systémy virtuální reality, kterým se předpovídá velká budoucnost, a to nejen v herním průmyslu, ale i v ostatních oblastech, např. v lékařství, ve stavebnictví či vědě. Prvním z realit je Augmented Reality (AR, rozšířená realita) fungující na počítačově vygenerovaném obrazu na již existujícím prostředí či předmětu prostřednictvím mobilního zařízení. Druhá je Virtual Reality (VR, virtuální realita), která je odlišná tím, že jsou zapotřebí speciální sluchátka a brýle, obraz je poté celý počítačově vygenerovaný. [42] Momentálně je nejvýznamnějším představitelem těchto systémů mobilní hra Pokemon GO od společnosti Niantic ve spolupráci s Nintenda. Hra dokázala za pouhý měsíc zvýšit tržby Nintendo, o 8 mld. dolarů na současných 40 mld dolarů, čímž předčila i dosavadního konkurenta Sony. [43] Virtuální a rozšířená realita budou v nadcházejících letech hlavními tématy herního průmyslu.

3.3 Videohra

Videohra je hra, která je založená na určitých pravidlech a povinnostech, některé mají také zakomponovaný rozvíjející se příběh. [44] Další definice zní, že videohra je určitý systém matematických vzorců a výpočtů. Avšak kdyby se videohra skládala pouze z matematiky, nebyla by možnost hrát videohry tak, jak je známo. [45] Videohry jsou v současné době vnímány jako interaktivní hry fungující na určitém softwaru a hardwaru (prostředkem je počítač, herní konzole či mobilní telefon). [46]

¹⁸ Rendering je proces vygenerování digitálního obrazu či objektu.

Pravidla videoher jsou různá, dle kategorie zaměření a prostředků hraní. V každé hře existují vstupy a výstupy [17], které se od hry ke hře liší. Mezi vstupy mohou být z hlediska lidských faktorů například inteligence, schopnost komunikace či obratnost a reflexe smyslů.

Komunikace a interakce jsou z hlediska hry rozděleny na dva způsoby. Existuje komunikace a interakce s NPC¹⁹ postavami, které jsou již předem naprogramované herními vývojáři a jejich úkolem je poskytnutí základních odpovědí a pomoci při řešení nejasností hráče. Další verze komunikace je skrz zabudované chat-systémy v hrách nebo přímá komunikace s jiným hráčem online. Také lze využít VoIP služeb při nedostupnosti či vylepšení komunikace, příkladem je již zmíněný Teamspeak. [36] Nedílnou součástí je interakce se samotnou videohrou, která závisí na herní platformě, viz kapitola 3.4.

3.3.1 Herní žánry

Herní průmysl má jako jiné zábavní průmysly několik žánrů, které se liší podle způsobu hraní a cíle hry. V následující tabulce (Tabulka 1) jsou vysvětleny jednotlivé herní žánry, které jsou doplněny nejvýznamnějšími herními tituly daného žánru hranými na počítačích. [47 str. 10]

Žánr	Popis
Akční	Akční hry jsou téměř všechny hry, ve kterých se hraje na základě boje. Proto další níže popsané žánry mohou být součástí akčního žánru, například bojové, RPG ²⁰ , střílečské, strategické a také závodní.
Bojové	K základním prvkům bojových her patří velký vstup tlačítek s cílem vytvářet kombinace útoků. Hry jsou typu 1 proti 1, ve kterých má každý z hráčů k dispozici stejné podmínky s jediným rozdílem, tím je výběr výjimečných postav. Nejznámější hry: Mortal Kombat, Street Fighter a Tekken.
Dobrodružné	Známé jako adventury, jsou to typy her silně založené na příběhu a plnění misí, také nesou některé prvky jako RPG hry (ukládání a vývoj postav). Tento žánr je určen především jednotlivcům, neboť hry jsou většinou graficky náročné a s dalšími vstupy ve formě online hráčů by zatížil počítač. Patří sem například hry Batman, Assasins Creed a God of

¹⁹ NPC – Non-player character

²⁰ RPG - Role playing game

	War.
MOBA ²¹	Nejspíše nejvíce rozvinutý herní žánr z hlediska sledovanosti (s milióny lidí sledujícími a hrajícími online). Principem těchto her je aréna, ve které hráči, většinou 5 proti 5, vylepšují svoji herní postavu s cílem dobýt a zneškodnit nepřátelský trůn. Tento žánr patří mezi akční a bojový, ale zejména nese prvky strategického. V profesionálních videohrách existují profese plnohodnotného herního kouče a manažerů týmů. Nejvýznamnějšími hrami moby jsou League of Legends, Dota 2 a Heroes of the Storm.
Puzzle	Hry tohoto typu jsou většinou nejméně náročné na požadavky hraní a znalostních vstupů. Základem her je úroveň náročnosti daného úkolu a postupně řešení dalších úrovní většinou pomocí logického myšlení. Takovými hrami jsou Bejeweled, Puzzle Quest a Portal.
RPG	Známky RPG jsou: hra založená na příběhu, velká mapa, hlavní postava, kterou lze levelovat a vylepšovat, forma oblečení a skillů, ²² dále jsou ukládány k dalšímu hraní. Online verze tohoto žánru je MMORPG, které bylo již zmíněno. V této podkategorii se hra zaměřuje na uskupení hráčů, také známe jako klany, zvané guildy ²³ , s cílem porážet konkurenci či splnění určitých misí. Hry offline: The Elder Scrolls, Fallout; a online: World of Warcraft, Guild wars a LineAge
FPS ²⁴	Známe také pod pojmem střílečky. Hry jsou většinou hrány z prvního pohledu hráče - v offline hrách splnění misí a v online verzi s cílem zneškodnit nepřátelský tým. Hry: Counter-Strike, Battlefield a Call of Duty.
Sportovní	Sportovní hry jsou založeny na konkrétním reálném sportu například fotbal, basketbal a další. Hru lze hrát většinou 1vs1, a to offline i online. Hry například FIFA, NBA a NFL.
Simulační	Simulační hry se dají označit jako virtuální činnost založená na reálné. Provádění operace, řízení auta, parkování, žití virtuální postavy atd. Hry

²¹ MOBA – Multiplayer online battle arena

²² Levelování je zvyšování úrovně herní postavy. Skillly jsou schopnosti herní postavy.

²³ Uskupení hráčů s pravidly a řádem. (Z herního hlediska)

²⁴ FPS - First person shooter

	jsou založeny na preciznosti odvedení „práce“. Patří sem The Sims, Euro Track Simulator a Surgeon Simulator.
Strategické	Strategické hry se jako akční hry vyskytují téměř u všech her, u kterých je požadována větší míra přemýšlení hráče, na základě toho je provedena akce. Hry jsou rozděleny do kol, každý z hráčů má určitý čas provést akci, poté se vystřídají. Patří sem Civilization, Warcraft a také karetní hry jako Hearthstone.
Závodní	Závodní hry spočívají převážně v závodech, které mohou být doplněny dalšími prvky jiných žánrů, ale v zásadě se celá hra zaměřuje na auto, nikoliv na postavu jako hlavního hráče. Nejznámější závodní hry jsou Need For Speed, Dirt, Gran Turismo a Super Mario Kart.
Ostatní	V poslední oblasti se vyskytují všechny zbylé herní žánry, které nejsou příliš hrány zejména z hlediska hráčské báze, kterou mají nejnižší. Patří sem žánry nesoucí formu tanečního, pěveckého či výtvarného prvku.

Tabulka 1 Žánry her, zdroj: Autor

Popularita žánrů je u každé platformy jiná, například u herních konzol se využívá herní analog, a proto mezi nejhranější hry patří bojové a dobrodružné. U osobních počítačů pak jde o střílečky a strategicko-akční hry, ke kterým je potřeba vysoká přesnost a velké množství vstupu hráče, čehož lze snadněji docílit klávesnicí a myší. U mobilních her se většinou jedná o jednodušší hry, které nespolehají na silnou grafiku, komplexnost a nejsou závislé na mobilním připojení. Mezi takové hry patří oddechové hry typu puzzle. Avšak v posledních letech je mobilní internet stále dostupnější, lze zaznamenat nárůst nových technologií, například celosvětový fenomén Pokemon GO, založený na AR.

Business modely videoher

Veškeré videohry jsou dále členěny podle způsobu zakoupení. Existují 3 základní business modely her. Tím prvním je F2P (Free-to-Play) neboli hra zdarma bez poplatků při stahování. Dalším modelem je B2P (Buy-2-Play), ke kterému je vždy jednorázově zakoupena hra ve formě digitální či fyzické kopie. Poslední možností zakoupení hry je měsíční předplatné P2P (Pay-2-Play), ve které je platba provedena bankovním převodem. Všechny tyto zmíněné způsoby mohou být dále rozšířeny za určitou peněžní částku. Nejčastějším

business modelem současné doby je F2P hra s placenými in-game službami a DLC rozšířeními.²⁵

3.4 Herní platformy a vybavení

Herní platformy jsou z hlediska hraní nejdůležitější, bez platformy nelze spustit žádnou hru. V dnešní době existuje celá řada poskytovatelů herních platform. K nejvýznamnějším patří konzolové od společností Playstation, Xbox a Nintendo. Z mobilní nabídky lze hry rozdělit podle vývojového prostředí pro Android a iOS. Poslední oblastí jsou počítače, které jsou z hlediska vytvořených her pro tuto platformu nejpočetnější. [48]

K platformám nezbytně patří i herní vybavení a periferie. K základnímu vybavení her na počítači patří klávesnice, myš, sluchátka a mikrofon, k těmto periferiím existují i speciální herní verze. Ke konzolám již tradičně patří herní analog, který může být rozšířen dle hry, například k závodní hře lze zakoupit herní volant nebo k tanečním hrám dokoupit kameru snímající pohyb či taneční desku. Mobily a smartphony nijak výrazné doplňky nemají, ale s růstem času tráveného na těchto zařízeních a vyšším využitím energie²⁶ se prodej powerbanek zvýšil. [49]

3.4.1 Struktura vývoje her

Vývoj her je proces, který je založen na účasti několika složek herního průmyslu. Záleží především na velikosti herní koncepce, která se liší od prvotřídních herních titulů po tituly jednotlivců a skupinek.

Z hlediska velkých herních vývojářů patří k prvnímu kroku vývoji her investice hardwarových společností, které mohou vyrobit speciální herní komponentu, například součástku k herní konzoli či u počítačů grafické karty. Další fází je samostatný vývoj her, který je buď finální v alfa, nebo beta fázi. Následuje publikace herního titulu a distribuce do obchodů. Poslední článkem je konečný zákazník, který může ovlivnit další průběh vývoje her, na což vývojáři reagují aktualizacemi a doplňky her. [18 str. 20]

Vývojový řetězec her



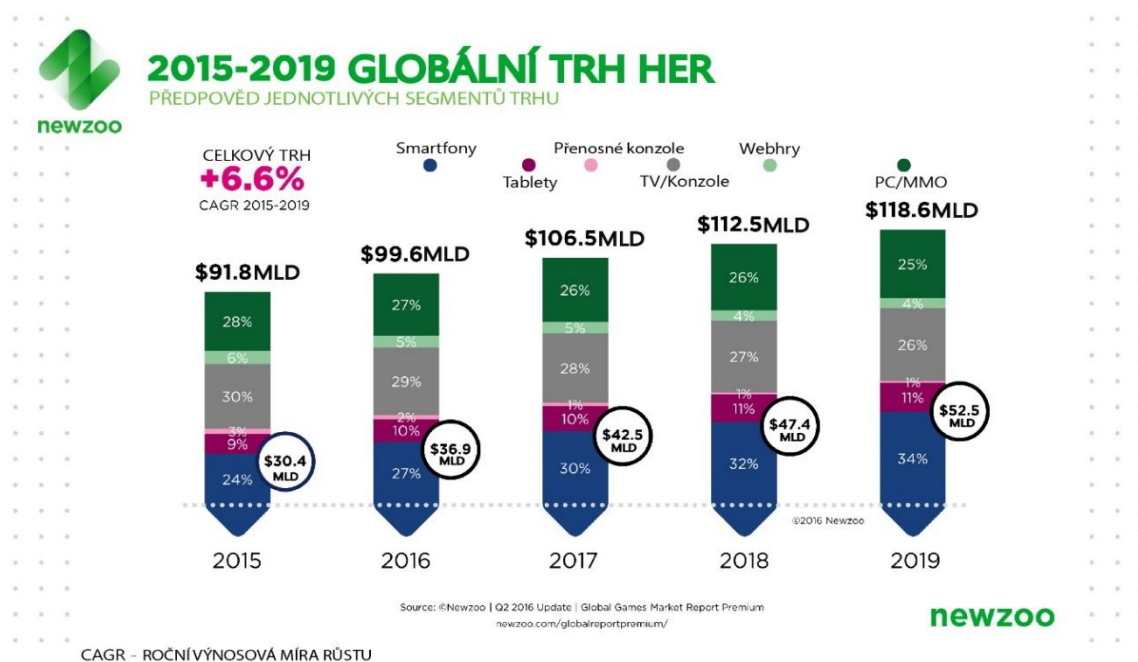
Obrázek 4 Vývojový řetězec her, zdroj: Autor

²⁵ DLC (Downloadable Content) je placené rozšíření hry.

²⁶ Nejvýznamnějším zástupcem Pokemon GO.

3.5 Trh herního průmyslu

Celkový trh herního průmyslu se dělí na tři základní druhy, které již byly zmíněny v předešlých kapitolách. Z nejvýznamnějšíchsem patří mobilní, počítačový a konzolový trh. Rozložení v herním průmyslu bylo v průběhu posledního desetiletí hodně obměněno. Níže je zobrazen graf (Obrázek 5) budoucího vývoje herního trhu, data jsou získána z webového serveru NewZoo, herního analytika herního trhu. [41]



Obrázek 5 Vývoj herního trhu [41], přeložil: Autor

Z obrázku je patrné, že mobilní trh bude nejvýznamnějším „hráčem“ následujících let. Není však překvapující, že právě mobily a zejména smartphony budou dominovat, neboť jsou dostupnější hlavně v rozvojových zemích. [50]

3.6 E-sports

E-sports, elektronický sport neboli sportovní soutěžení hráčů videoher je v současnosti jedním z fenoménů a snem mnoha dospívajících ze všech koutů světa. E-sport lze považovat za tradiční sport, ke kterému existuje organizace, management, trenér a smluvní podmínky hráčů, reklamní kampaně a další náležitosti.

Turnaje

Nedílnou součástí elektronického sportu jsou turnaje jednotlivých her. K nejvýraznějším turnajům z hlediska finančních odměn, marketingu a celkového vývoje jsou hry Dota 2 a League of Legends. Obě tyto hry jsou druhem MOBA, dále FPS hra Counter-Strike:

Global Offensive (CS:GO) a Overwatch.²⁷ [51] Tyto turnaje se konají jednou, někdy i několikrát do roka, a to buďto online, nebo LAN - živě před publikem.

Příkladem je turnaj s názvem „The International“, který organizuje každoroční mistrovství hráčů hry Dota 2 s 16 kvalifikovanými týmy z celého světa. První turnaj byl v roce 2011 a tehdy se hrálo o největší sumu doposud, 1,6 mil. dolarů. [52] Letos proběhl 6. ročník tohoto turnaje a během doby se z původních 1,6 mil hraje o 21 mil. dolarů z celkových 87 mil. za všechna období. [53]

Hráči

V současné době jsou v některých zemích považováni počítačová hráči za plnohodnotné sportovce zavázané smlouvami organizací a reklamním společnostem. Každý z profesionálních hráčů má svoji fanouškovskou základnu, se kterou komunikuje prostřednictvím sociálních sítí nebo streamovacími službami, jako je např. Twitch.tv. Příjem hráčů není nijak omezen a lze vydělávat právě na těchto komunikačních nástrojích, v nichž fanoušci darují peníze či se přihlásí k měsíčnímu předplatnému zvýhodněných služeb. Nejznámější osobou v herním průmyslu a také nejvíce sledovanou osobou na Youtube je PewDiePie²⁸ s téměř 50 miliony odběratelů.

Věk e-sportovců je velmi důležitým aspektem, neboť mnoho her závisí na lidských reakcích a akcích provedených za minutu.²⁹ S vyšším věkem nelze dosáhnout takových výkonů, které by byly na standardní úrovni. Úspěšní hráči, kteří si prošli touto proměnou, skončí buď jako trenéři, či zůstanou s herním průmyslem spojeni jako herní analytici, komentátoři. Stát se profesionálním hráčem nese také mnoho rizik, neboť rozmezí 15-25 let je optimální věk hráčů, a proto se mnozí musí většinou vzdát středního či vysokoškolského vzdělání; případně ho odsunout. Záleží však na žánru her.³⁰ [54] Níže je poskytnut náhled na nejvýdělečnější hráče v profesionálním hraní her.

²⁷ Součet aktivních hráčů zmíněných her tvoří téměř 100 milionů.

²⁸ 27letý Švéd, celým jménem Felix Arvid Ulf Kjellberg.

²⁹ Známé jako APM (Actions per minute).

³⁰ Rozdíly mezi akčními, na reakcích založenými hrami a strategickými hrami, kde je potřeba jen přemýšlet.

Nejvyšší zisky (celkově)					
	Přezdívka	Jméno hráče	Celkový zisk	Hra	Zisk (ze hry) % z celku
1.	UNiVeRsE	Saahil Arora	\$2,629,645.24	Dota 2	100.00%
2.	ppd	Peter Dager	\$2,618,120.36	Dota 2	99.38%
3.	Fear	Clinton Loomis	\$2,383,155.64	Dota 2	99.94%
4.	Sumail	Sumail Hassan	\$2,310,447.74	Dota 2	100.00%
5.	iceice	Li Peng	\$1,939,979.63	Dota 2	100.00%
6.	Aui_2000	Kurtis Ling	\$1,898,028.64	Dota 2	100.00%
7.	bLink	Zhou Yang	\$1,896,430.02	Dota 2	100.00%
8.	Innocence	Zhang Yiping	\$1,896,430.02	Dota 2	100.00%
9.	Faith_bian	Zhang Ruida	\$1,896,369.60	Dota 2	100.00%
10.	Shadow	Chu Zeyu	\$1,896,269.60	Dota 2	100.00%
11.	xiao8	Zhang, Ning	\$1,788,244.53	Dota 2	99.58%
12.	Hao	Chen, Zhihao	\$1,759,847.03	Dota 2	99.63%
13.	Mu	Zhang, Pan	\$1,390,711.91	Dota 2	99.69%
14.	Puppey	Clement Ivanov	\$1,333,926.36	Dota 2	99.92%
15.	Banana	Jiao, Wang	\$1,279,561.56	Dota 2	99.06%
16.	MiSeRy	Rasmus Fillipsen	\$1,254,109.32	Dota 2	99.94%
17.	SanSheng	Wang, Zhaohui	\$1,207,649.37	Dota 2	99.27%
18.	MMY!	Lei, Zengrong	\$1,112,556.41	Dota 2	98.89%
19.	Zai	Ludwig Wåhlberg	\$1,093,469.44	Dota 2	98.29%
20.	Fenrir	Lu, Chao	\$1,087,957.78	Dota 2	100.00%
21.	w33	Aliwi Omar	\$1,078,930.78	Dota 2	100.00%
22.	iceiceice	Koh, Daryl Pei Xiang	\$1,073,865.96	Dota 2	99.78%
23.	KuroKy	Kuro Takhasomi	\$1,024,520.95	Dota 2	99.93%
24.	Sylar	Liu, Jiajun	\$994,169.82	Dota 2	99.39%
25.	Super	Xie, Junhao	\$981,292.93	Dota 2	98.04%
26.	fy	Xu, Linsen	\$956,343.94	Dota 2	100.00%
27.	s4	Gustav Magnusson	\$951,347.08	Dota 2	99.89%
28.	LaNm	Zhang, Zhicheng	\$906,950.13	Dota 2	99.95%
29.	Faker	Lee, Sang Hyeok	\$896,596.98	League of Legends	100.00%
30.	Arteezy	Artour Babaev	\$888,675.61	Dota 2	100.00%
31.	Resolution	Roman Fominok	\$877,585.75	Dota 2	100.00%
32.	NOtail	Johan Sundstein	\$843,651.16	Dota 2	99.03%
33.	Bengi	Bae, Seong Ung	\$809,461.00	League of Legends	100.00%
34.	Agressif	Sun, Zheng	\$790,034.66	Dota 2	100.00%
35.	Mushi	Chai, Yee Fung	\$771,700.02	Dota 2	99.96%

Obrázek 6 Nejvíce vydávající hráči, zdroj [53], přeložil: Autor

Největší zastoupení je hráčů Dota 2, kteří inkasovali nejvíce peněz z video her. Jedná se většinou o vítěze a semifinalisty každoročního turnaje „The International“, který byl výše popsán výše.

3.7 *Sponzoři a partneři*

Sponzoři jsou nedílnou součástí herního průmyslu. Zásobují zejména profesionální týmy finančně i věcně za splnění určitých podmínek. Sponzorovat lze také turnaje, významné osobnosti herního průmyslu, významné herní akce či samotné hráče. Mezi sponzory herního průmyslu patří zejména společnosti, které jsou součástí počítačového světa, například společnosti grafických karet Intel, Nvidia, výrobci počítačů Dell, Msi, online streamingové platformy Twitch.tv a Azubu. Avšak patří sem i jiní netradiční sponzoři, například výrobce energetických nápojů Monster, herních židlí Need For Seat a oblečení GamersApparel. [55] [56] Dalšími významnými partnery jsou online trhy s videohrami a virtuálními předměty z her.

Ke sponzorům a partnerům patří i online sázkové služby. Jako u běžných sportů i zde existuje řada služeb poskytujících kurzy na výherní týmy, ve kterých lze sázet virtuálními penězi, virtuálními věcmi a také reálnými penězi.

4 PHISHING A SCAMMING VE VIDEOHRÁCH

Herní prostředí je ideálním místem pro zloděje virtuálních věcí, peněz a osobních údajů. Za prvé nejsou zde zábrany z hlediska fyzické náročnosti zloděje, za druhé způsoby krádeže nejsou nijak složité. I když jsou proti online krádežím herní servery zabezpečeny, u běžného phishingu a dalších podvodných metod je hlavním faktorem lidská schopnost a zkušenost rozpoznat situaci, přičemž dohledatelnost těchto zločinců je téměř nulová. Tato kapitola je rozdělena následovně:

- Kultura her;
- Podvody;
- Černý trh (Komunita, prodej a zneužití);
- Porovnání odlišností s běžným phishingem.

4.1 Kultura her

Hry jsou většinou bezbariérové a téměř kdokoliv může komunikovat s kýmkoliv. Ve hrách se lze setkat s lidmi z jiných kontinentů, nejrůznějších národů a jazyků. Přestože existuje taková různorodost, hry umožňují komunikaci v angličtině, neboť téměř všechny hry vycházejí v anglických verzích.³¹ Výjimkou mohou být asijská vývojová studia, která se zaměřují jen na místní komunitu. Za zmínku stojí jihokorejské společnosti, které dominují a považují hry za součást života běžného i profesního. [54]

4.2 Podvody

Existuje mnoho metod krádeží virtuálních věcí a peněz v hrách. Všechno je zapříčiněno nedbalostí a jednáním jedince v časové tísní. Nejběžnější metodou podvodů je za pomoci nelegálních reklam a doplňkových služeb třetích stran přímo prostřednictvím her. Takovým herním postavám se říká spamboti. Jsou to automatizované herní postavy vytvořené za účelem nalákat oběti na falešné stránky. Každá hra má jiný charakter, ke kterému lze vždy najít nějaký druh online podvodů. Příkladem mohou být vylepšení výzbroje, cheaty³², zrychlení hry a další nelegální rozšíření.

Avšak záleží na druhu platformy, kde se hra hraje a jakého je žánru. Z mobilního hlediska jsou podvody zaměřeny zejména na internet, kdy na hře vyskočí reklama na jiné hry či dokoupení doplňku pro danou hru. U některých mobilních her je tento způsob součástí

³¹ Výjimky mohou nastat u asijských her, které jsou vyvíjené jen pro danou zemi.

³² Cheat je užívání doplňkových nelegálních aplikací v hrách nebo herní rozšíření, které umožňuje vynechat určitá pravidla hry.

obchodování, kdy hry jsou F2P, ale obsahují mnoho nedostatků a je potřeba zakoupit doplňky, které jsou pro uživatele předražené až nevýhodné. [57]

V MMORPG hrách je běžné za finanční částku prodávat herní postavy, které lze dnes prostřednictvím internetových obchodů, jako je eBay, zakoupit. [58] Prodávají se samostatně účty postav určité hry, které jsou výjimečné například obsahem inventáře či zvládnutých úkolů v dané hře anebo virtuálních věcí. Je velmi složité zkontrolovat, zda poskytnutý herní účet obsahuje to, co nabízí, proto kupující musí být seznámen s obchodními a smluvními podmínkami zprostředkovatele. Podvodník může být prodávající, ale i kupující, využívají se klamavé informace z hlediska prodávajícího a z pozice kupujícího lze podvod uskutečnit s falešnými sliby, splácením a nákupem účtu či jiných herně souvisejících věcí. [59]

Základním opatřením proti těmto podvodům je dostatek informací, jako je seznámení se se situací, herní znalost, smluvní podmínky a reference dané osoby.

4.3 Černý trh

Černý trh je v herním průmyslu nelegální hospodaření virtuálních prostředků a věcí, zejména kradených od jiných uživatelů s cílem dosáhnout zisku. Níže je přiblížena komunita černého trhu a její obchodování.

4.3.1 Komunita

Existuje několik diskuzí a fór, v nichž se shromažďují zlodějové a překupníci virtuálních věcí do her a herních účtů. Pro příklad je zvoleno jedno herní fórum nabízející tyto služby, jedná se o německou stránku www.elitevpers.de. [60] I když se zde prodávají herní účty jednotlivých her pod určitým uživatelským jménem, nelze vždy rozeznat původ těchto účtů, neboť se prodávající vydávají za původní majitele, aby neporušili smluvní pravidla a zároveň snížili dopadení ukradených účtů. Kupující kupují herní účty ze dvou hlavních důvodů, kterými jsou lenost vlastního levelování postavy nebo slouží jako náhradní herní účet k dalším účelům³³, tyto situace jsou nejčastěji využity v hrách typu MMORPG.

4.3.2 Prodej a zneužití

V těchto herních fórech se prodává velké množství herních položek, k nejvýznamnějším patří herní účty, jak je již výše zmíněno, nebo uskutečnění prodeje virtuálních peněz v hrách MMORPG, které nejsou vždy poctivě vydělány. [60] Příkladem může být bot, herní postava, která dokáže sama sbírat virtuální peníze. Může být i naprogramovaná, aby

³³ Podpora virtuální postavy kupujícího nebo slouží k dalšímu prodeji či zneužití pod jménem zakoupeného účtu.

plnila úkoly v online hrách. Poslední obchodovatelnou položkou her jsou virtuální věci, kterými lze docílit krádeží z jiných účtů, či využití nelegálních aplikací k vygenerování dané věci.

Prodávají se zde i programy, kterými si lze zjednodušit hru, jsou však nelegální a často jsou tyto herní účty zabanovány. Jedná se o boty všech druhů a funkcí s cílem ulehčit si hru.³⁴

4.4 Porovnání odlišností s běžným phishingem

Hry jsou jedinečné tím, že největší zastoupení hráčů je z věkové kategorie mladiství či dorost, která právě napomáhá útočníkům a zlodějům využít jejich nezkušenost s podvody, neboť oproti obecným phishingovým metodám, které jsou zaměřeny převážně na dospělé pomocí falešných e-mailů a ve kterých jsou zahrnuta zejména témata jako bankovní situace či nabídka zabezpečení údajů [61], se v herním prostředí zaměřují na falešné nabídky k vylepšení konkrétní hry a in-game služeb. Dále se při hrách jednodušeji naváže kontakt mezi hráči, jedinou podmínkou je společný jazyk a hra, kterou oba hrají.

Oproti běžným phishingovým e-mailům se phishing ve hrách zaměřuje na krádeže herního účtu, nikoliv platebních karet a údajů, které mohou být sekundární důvod.

³⁴ GoldBot – automatický sběr virtuálních peněz ve hrách
FarmBot – automatické hraní postavy a plnění úkolů
AimBot – automatické zaměření na cíl v hrách FPS

5 DRUHY ÚTOKŮ PHISHINGU

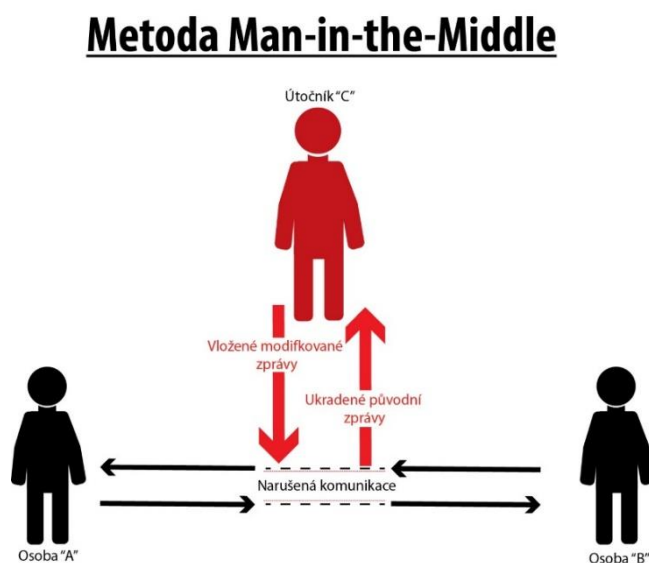
Každý phish má svou metodu provedení. V následující kapitole jsou podkapitoly členěny dle tří nejčastějších metod útoků z obecného hlediska. Na začátku je stručně popsána metoda Man-in-the-Middle, která souvisí se všemi dalšími útoky popsány níže.

- Man-in-the-Middle;
- Falešná identita;
- Přesměrování;
- Vyskakovací okna.

5.1 *Man-in-the-Middle*

Útok Man-in-the-Middle (MITM) spočívá v odposlouchávání a narušení komunikace mezi dvěma stranami útočníkem. [1] Existuje několik případů, u kterých lze toto zneužít. Příkladem mohou být rozhovory mezi klientem a odborníkem, kdy se útočník chová jako odborník, ale ve skutečnosti získává informace sdělené původním odborníkem. Tímto způsobem funguje takzvaná metoda falešné identity.

Jako příklad lze popsat následující situaci. K dispozici jsou dvě osoby „A“ a „B“ komunikující mezi sebou a třetí osoba „C“ je útočník. Komunikace probíhá na Skypu a útočník má obě osoby uložené jako falešná „A“ a „B“, ale skutečná „A“ a „B“ mezi sebou nikoliv. „A“ podává otázky osobě „B“, která je ve skutečnosti „C“. Ta situaci zneužije a „B“ píše zprávu „C“, která měla být původně od „A“. Takhle pokračuje další výměna zpráv, dokud neskončí či dokud útočník nezíská potřebné informace k nelegální činnosti. (Obrázek 7)



Obrázek 7 Metoda MITM, zdroj: Autor

5.2 *Falešná identita*

Metoda falešné identity je nejběžnějším útokem phishingu. K docílení úspěšného útoku je zapotřebí minimum počítačových zkušeností webového jazyka html, css, php, javascriptu a další. Nejdůležitějším aspektem tohoto útoku je takzvané zrcadlení webové stránky. Princip spočívá v kopírování webu z hlediska grafiky a úpravy html kódu. Výsledná webová stránka bude identická s původní, jen s rozdílem webové adresy, kterou lze vytvořit na free server hostingových stránkách³⁵.

Prostředkem pro šíření phishingové stránky je elektronická komunikace, a to v různých formách. Nejvíce jsou zneužívány e-maily, protože jsou největší z hlediska objemu užívání. Dalším způsobem je přímé kontaktování z některých sociálních sítí, kdy se útočník maskuje pod osobou či organizací, kterou oběť zná.

Mezi podvodná témata těchto stránek patří banky, pojišťovny a další finanční instituce, ve kterých se útočník zaměřuje na vykrádání bezhotovostních finančních prostředků oběti.

5.3 *Přesměrování*

Phishingový útok pomocí přesměrování funguje téměř na stejném principu jako u falešné identity pouze s jediným rozdílem, že odkaz, který útočník sdílí, je skutečný, ale oběť je v průběhu přesměrování na konkrétní stránku okradena o své údaje, poté se však vyskytne znova na skutečné stránce. Oproti metodě falešné identity je tato metoda sofistikovanější, protože k útoku není potřeba zrcadlení, ale úprava stávajícího webového kódu za cílem nejmenšího zásahu.

Tato metoda se nejčastěji používá u internetových obchodů, které pravidelně rozesílají své reklamy a akce na zboží prostřednictvím e-mailu, protože tímto způsobem nevzbudí u oběti takovou pozornost jako u náhodného e-mailu, který se pravidelně neobjevuje. Oběti jsou také u těchto marketingových tahů zvyklé, že budou po kliknutí na odkaz přesměrovány. [1 str. 61]

5.4 *Vyskakovací okna*

Tento phishingový útok je ze zmíněných nejméně běžný, neboť v dnešní době má nejnižší realizaci úspěšného útoku. Současné webové prohlížeče již mají několik zabudovaných nástrojů k zablokování nezvaných a nekvalifikovaných pop-upů. [1 str. 64]

³⁵ Placené či neplacené webové servery, které umožní uživatelům nahrát si jejich webovou stránku.

Principem útoku je zaslání skutečného odkazu (jako u předešlých metod), ale s tím rozdílem, že po kliknutí je oběť vyzvána k zadání přihlašovacích údajů pomocí vyskakovacího okna a následně jsou ukradené informace doručeny útočníkovi.

6 MOŽNOSTI OCHRANY

Proti phishingovým útokům existuje celá řada bezpečnostních opatření. Informace a osobní údaje, které jsou hlavním cílem útočníků, je potřeba střežit jako peníze a je nutné zajistit k nim patřičná opatření.

Důležitým krokem je rozpoznat podvod phishingových stránek a útoků a vyhnout se jim. U phishingových e-mailů si je nutné ověřit odesílatele, jejich obsah a odkaz webové stránky. Následující upozornění, které se musí vždy dodržet pro bezpečné surfování po internetu: „*Nikdy nevypisovat žádné osobní ani přihlašovací údaje do předem neověřených stránek.*“ [62]

Z toho vyplývá, že nejdůležitější obranou proti phishingu je opět lidská schopnost rozpoznat phish. V následující kapitole provedu nejvýznamnějšími nástroji zabezpečení se základními pravidly proti phishingu:

- Antiviry;
- Autentizace;
- Black list;
- Anti-phishingové aplikace;
- Shrnutí.

6.1 Antiviry

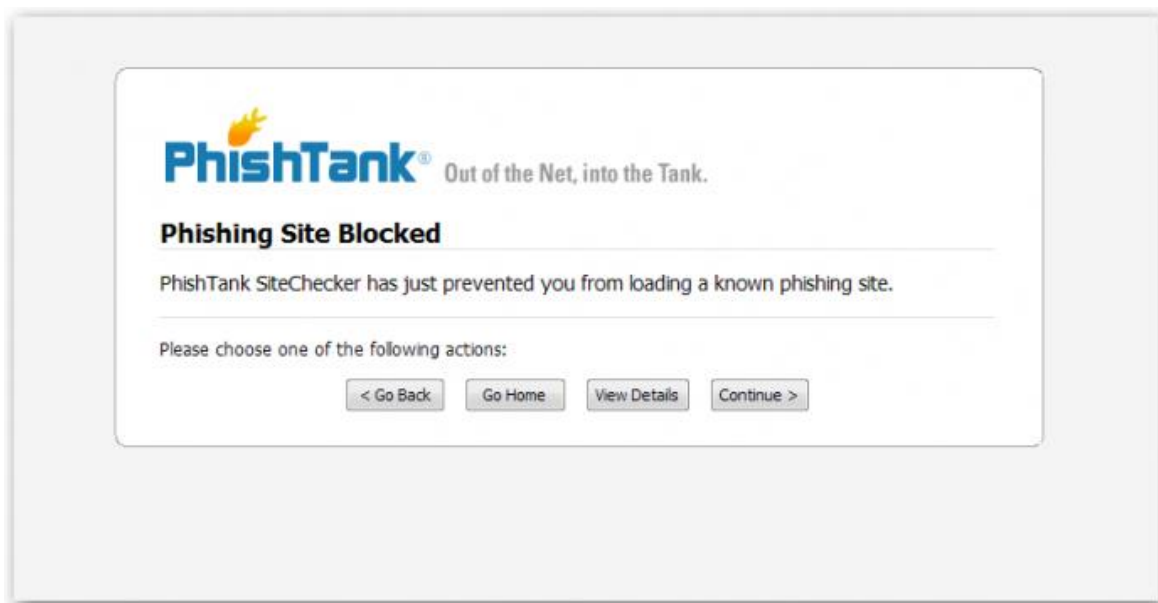
Ochrana ve formě antivirů je jednou z nejzákladnějších metod opatření proti kyberútokům. Antivirus je software, který zabráňuje nezvaným a nebezpečným softwarům na počítači, malwarům, ale také webovým malwarům, mezi které patří spamy, scamy a phishingové útoky a maže je. Je nutné mít vždy aktualizované antivirové softwary a jejich licence, neboť útočníci nikdy nezůstávají u stejných metod, stále je rozvíjí.

Mezi nejznámější antiviry na trhu patří Norton, Avast, ESET a AVG, všechny tyto antiviry mají verzi ke stažení zdarma, i když jsou velmi omezené. Doporučené je přikoupit si doplňky jednotlivých společností, které se pohybují v cenovém rozmezí 600-1000 Kč na rok. [63]

V roce 2016 provedla nezávislá testovací společnost antivirů AV anti-phishingový test pomocí tří antivirů (Bitdefender, ESET a Kaspersky) na 500 phishingových stránkách bankovních institucí různých zemí. Průměrná úspěšnost všech byla 92 % zablokovaných stránek. [64]

6.2 Anti-phishingové softwarey

Existuje mnoho anti-phishingových softwarů, které mohou být integrovány ve webovém prohlížeči uživatele či nainstalovány externě na počítači. Fungují na stejném principu jako antiviry, kdy hledají nedůvěryhodné údaje a upozorní uživatele na tyto události. Nejběžnější postup těchto softwarů je vyskakovací okénko, které nás upozorní na nebezpečný obsah webové stránky. PhishTank SiteChecker a GFI Mail Essentials patří mezi nejznámější v této oblasti.



Obrázek 8 Ukázka blokace jednoho z phishingových webů, zdroj: Autor

6.3 Blacklist

Takzvaný Blacklist je seznam nebezpečných a nežádoucích webových stránek jednotlivých bezpečnostních serverů, které je zveřejňují prostřednictvím internetu.³⁶ V seznamu je vždy oznámeno, o jakou IP adresu se jedná a odkud pochází, doložen je důkaz nebezpečného chování stránky pomocí logů antivirů s popisem, o jakou hrozbu se jedná. (Obrázek 9)

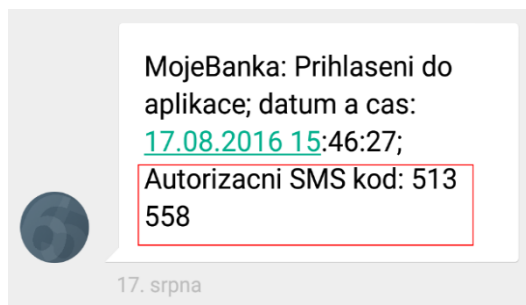
³⁶ Dále existují Whitelisty a Greylisty, obě jsou mírnější obdoby Blacklistu.

Date	Domain	IP	CC	ASN	Autonomous System Name	Click Mds for VirusTotal Report
2016-10-24	amenogo.professor979.ru/clicker_new_dis.exe?etag=d306caed10dcb0586d96a010d75f3b	82.118.16.164	UA	15626	ITLAS, UA	e529fd0fb996a8ca72e39d9b0b802b97
2016-10-24	cdn.bispd.com/mirror/foodbuzz/FoodBuzzInstaller.exe	78.138.126.82	DE	25074	INETBONE-AS MESH GmbH	abd9e9d862e3a355d469d05297276bdd
2016-10-24	down.mirosoftup.com/down/2.exe	59.188.68.200	HK	17444	NWT-AS-AP AS number for New World Telephone Ltd., HK	7ef04a0cd91b01dd3d08a3bea3d9632d
2016-10-24	limlim00000.rozup.in/senario104.jpg	79.127.127.67	IR	43754	ASIATECH-AS Asiatech Data Transfer Inc. PLC,IR	7714fcd2d8f60a76f2f77ba56666437
2016-10-24	pf.dlovit.com/s/7/9/79396-660945-blueexpand-bluetooth-file-manager.exe	149.202.192.156	FR	16276	NA	3b0a8a947ddefe22c4b8d863906855d
2016-10-24	sqiuba.176win.com/176Win.exe	219.84.168.195	TW	18182	SONET-TW Sony Network Taiwan Limited,TW	4f04423e84f839ee40e244b124e0e1c
2016-10-24	upstreams.info/wp-admin/includes/pm.dll	72.167.232.34	US	26496	PAH-INC - GoDaddy.com, Inc.	3c4de20e484146bec844471867bd1628
2016-10-24	www.awkinstalls.com/roib/update2.exe	174.137.173.70	US	27257	WEBAIR-INTERNET - Webair Internet Development Company Inc.US	fd97b8646752090ef23305528ec8fb6
2016-10-24	211.45.30.136/updatefb/autoclaimfile/CL_AutoClaimEst_Mgmt.exe	211.45.30.136	KR	6619	SAMSUNGNETWORKS-AS-KR Samsung Networks Inc.	6d018c3d0e1bc177957a552407cd9f54
2016-10-24	az745681.vo.msecnd.net/downloadguides/e7e12d9d-a7b9-4e36-b817-cd0754ae4b1/pantsoff.exe	72.21.81.200	US	15133	EDGECAST - EdgeCast Networks, Inc.US	e37e180a7935e408392e2a9f9f659337
2016-10-24	d11m2p9mpffp32.cloudfront.net/main/web_zt.exe	52.84.125.61	US	16509	NA	e04e30707b79d4f69a30fb0b301d6f7
2016-10-24	downloads.tweakbit.com/en/river-updater/default/stub/autodriver-updater-setup.exe	45.79.194.109	US	3595	GNAXNET-AS - Global Net Access, LLC.US	a77389f9b1f74566e0d728b217bc31ab
2016-10-24	onaparti.unitdriveway.ru/nethost.exe	46.28.67.156	UA	15626	ITLAS, UA	78c9e8f51994a7af369db5a9edcd0f9
2016-10-24	rdovicia.hookresearch.ru/video/plugin_win7_.exe	46.28.67.156	UA	15626	ITLAS, UA	6b05c8e45e7bc90806cd02e04379e4a
2016-10-24	update.xunyou.com/xunyou2014/uninstall_20161023.exe	203.130.54.225	CN	54994	QUANTIL - QUANTIL, INC. US	9f6eb3948d7941cd0b7501cd6b6f93
2016-10-24	url.d9soft.com/down/QQ1.exe	222.186.161.72	CN	23650	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone, CN	931679df2703ea3ac1db37cfafe88a4
2016-10-24	www.froggie.sk/download/Vistalizer.exe	92.240.253.14	SK	42005	LIGHTSTORM-COMMUNICATIONS-SRO-SK-AS LightStorm Communications s.r.o.	ae423f31ce0d0167109af2416e3e09f
2016-10-24	103.234.36.75/rd927.exe	103.234.36.75	VN	45638	QOS-AS-VN Online data services, VN	9825e7c60ddbeff7f08fb0cae2b1200b6
2016-10-24	allitri.professor979.ru/clicker_new_ru.exe?etag=2f9dac9191ad2763f79081c3399b1a04	82.118.16.164	UA	15626	ITLAS, UA	b5be2edd5fe3d14cd8a477537830a4566

Obrázek 9 Seznam nebezpečných stránek ze serveru www.malc0de.com [79]

6.4 Dvufaktorová autentizace

Jde o jeden ze způsobů, který umožní vysokou bezpečnost proti phishingovým nástrahám. Dvufaktorová autentizace je ověření totožnosti uživatele na základě více nástrojů současně. K nejběžnějším způsobům patří e-mailová nebo mobilní verifikace uživatele. Princip funguje tak, že k úspěšnému přihlášení je nutné přidat kód, který byl zaslán k jedné z výše zmíněných možností. (Obrázek 10)



Obrázek 10 Autentizace u KB pomocí SMS, zdroj: Autor

6.5 Shrnutí

Ne vždy se lze ubránit proti phishingu pomocí bezpečnostních aplikací, nejdůležitější je schopnost uživatele rozpoznat phish a náležitě na něj zareagovat. Další nevýhodou bezpečnostních aplikací je cenová dostupnost, neboť obecně placené aplikace jsou rozšířené o vyšší bezpečnostní nástroje než verze zdarma. Mnoho aplikací zároveň zatěžuje výkon počítače, neboť bezpečnostní programy musí být vždy spuštěny k docílení maximálního zabezpečení. Výhodou všech aplikací ale je, že téměř vždy upozorní uživatele na technické útoky na soubory a systémové složky.

7 ANALÝZA HERNÍ PLATFORMY STEAM

Analytická část je rozdělena na tři kapitoly. První se věnuje analýze herní platformy Steam s aktuálním trhem a SWOT analýzou, ve druhé jsou vybrány útoky, se kterými se lze setkat na Steamu, v poslední jsou popsána bezpečnostní opatření na Steamu se závěrečným vyhodnocením analyzovaných útoků,

- Steam (Úvod, platforma);
- Působíště na trhu (Celosvětové zastoupení, americký a český trh);
- SWOT analýza.

7.1 STEAM

7.1.1 Úvod

„The ultimate entertainment platform.

Play, connect, create and more.

Install Steam today and start gaming!“ [65]

Steam je herní multifunkční platforma vyvíjená společností Valve Corporation založená v roce 2003. Komunita na Steamu se skládá zejména z hráčů videoher, designérů virtuálních věcí a prostředí. Početnou součástí komunity jsou herní vývojáři, kteří prostřednictvím Steamu mohou inzerovat svoje hry, a to od malých a nenáročných až po hry celosvětového formátu.

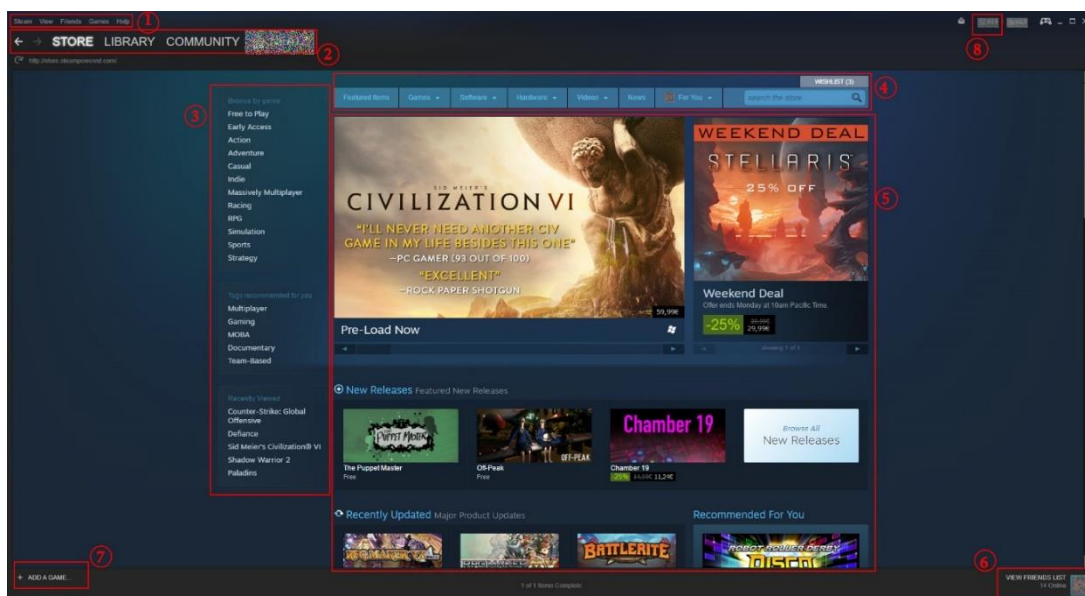
7.1.2 Platforma

Platforma Steamu poskytuje kromě nakupování her mnoho dalších možností, jako jsou diskuzní fóra, online streaming platforma, vlastní hudební přehrávač, vlastní knihovna her, obrázků a videoklipů, možnost přepnutí na televizní mód/vzhled a v neposlední řadě vlastní Steam klient, na kterém všechny zmíněné funkce lze spustit.

V průběhu několika let se vzhled a funkce Steamu hodně změnila, v současnosti se vyvíjí nejnovější trend, kterým je virtuální realita. Steam poskytuje vlastní hardware SteamVR, ke kterému je již vyvinuto několik stovek her od různých herních vývojářů.

Níže je zobrazena úvodní stránka, které poskytuje informace o hrách nabízených v současné době. Steam je známý svými sezónními akcemi³⁷ na vybrané hry, které jsou někdy zlevněny až o 90 % a ve výjimečných případech jsou placené hry na určitou dobu zdarma ke stažení.

³⁷ Lépe známe pod anglickým názvem Steam Sales.



Obrázek 11 Ukázka Steam klientu, zdroj: Autor

Vzhled Steam klienta je členěn do několika sekcí, avšak v tomto případě vyberu jen ty nejdůležitější pro další zorientování.

1. Navigační panel – Administrativa účtu, klientu a her + podpora
2. Hlavní panel – Obchod, knihovna her, komunita Steamu a vlastní profil
3. Postranní panel – Doporučené a nejznámější herní žánry
4. Nabídka her a aplikací – Specifičtější výběr her a aplikací dle potřeb
5. Úvodní stránka – Aktuální herní nabídky a slevy
6. Uživatelský účet – Seznam přátel (Obrázek 12)
7. Další možnosti rozšíření – Přidání libovolných her a aplikací do Steamu
8. Finanční balance účtu – Pro většinu zemí EU je měna v eurech³⁸



Obrázek 12 Zmenšený
Steam klient s přáteli
a skupinami online, zdroj:
Autor

Vlastní profil na Steamu obsahuje údaje o úrovni na Steamu, které se zvyšují při nakoupení her přes platformu, dále obsahu-

³⁸ Dalšími měnami jsou například: americký dolar, britská libra, švýcarský frank a další. Bohužel česká koruna není stále na seznamu.

je čas posledního hraní. Při vyšších úrovních Steamu lze modifikovat vzhled vlastního profilu, který je významný jen z estetického hlediska.

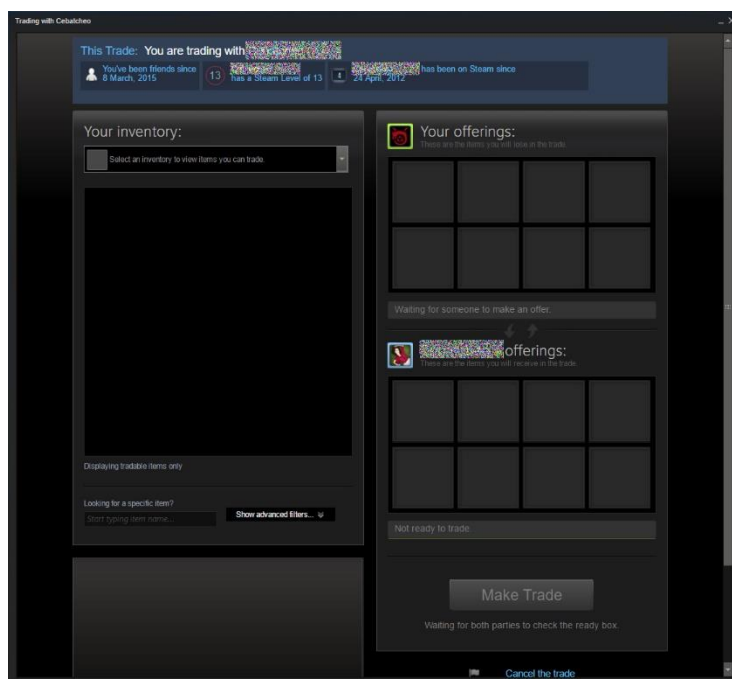
Možnosti klientů jsou více členěny, ale z hlediska obsáhlosti jsem k dalšímu postupu práce, které popíšu níže, vybral jen nejdůležitější nástroje Steamu.

7.1.3 Steam obchod a chat

Mezi zvoleným nástroji jsem si vybral komunikační prostředek Steam chat, který umožňuje běžnou komunikaci na Steamu mezi přáteli a zapíná se pomocí zmenšeného klienta Steamu (Obrázek 12).

Pomocí klienta lze pozvat hráče ke hře, do skupin, do větších konverzací a v neposlední řadě k obchodu s virtuálními věcmi. Při obchodu se otevře okno s věcmi uživatele všem obchodovatelným věcem na Steamu a místo pro vkládání, a to od nabízejícího a příjemce.

V okně se objevují důležité informace o druhé osobě (datum sprátení, stáří a úroveň Steam účtu) (Obrázek 13)



Obrázek 13 Steam trade, zdroj: Autor

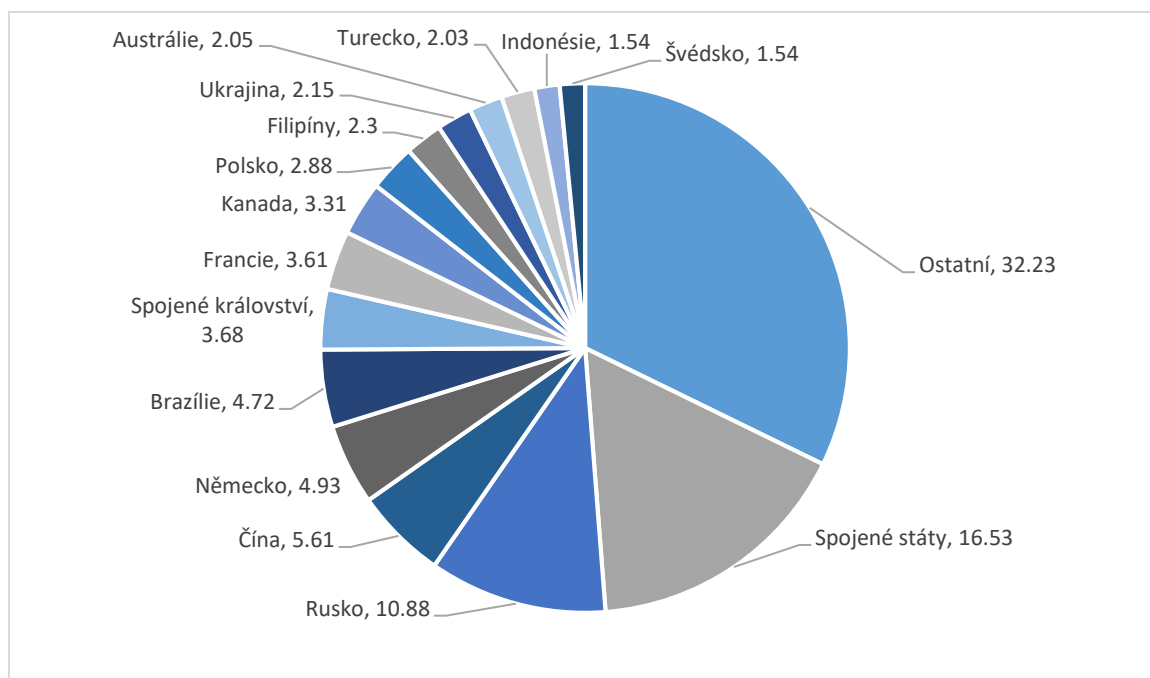
Tyto dva nástroje budou nedílnou součástí k porozumění dalšího zpracování práce.

7.2 Působíště na trhu

Steam je celosvětový poskytovatel digitálních her, které jsou v každé zemi jinak rozděleny dle oblíbenosti a počtu stáhnutí konkrétního herního titulu. V této analýze se zaměřím na celosvětové zastoupení zemí, postavím americký trh proti českému, tato data zpracuji do grafů a tabulek získaných z webové stránky specializující se na analýzu Steamu www.steamspy.com [66] a www.steamcharts.com [67].

7.2.1 Celosvětové zastoupení

Uživatelé Steamu



Obrázek 14 Steam uživatelé dle státu ke dni 21. 10. 2016 v procentech, zpracoval: Autor

Největší zastoupení hráčů je ve Spojených státech, neboť herní průmysl je zde nejvíce rozvinutý a také nejdostupnější ze všech zemí. Následuje Rusko a další evropské země. Jedinou významnou asijskou zemí je Čína, i když je to poněkud zvláštní, neboť řada her je založena pro asijskou společnost, zejména hry MMORPG, nebývá součástí Steamu. Uživatelé z Asie většinou vlastní jen jedinou hru, kterou je Dota 2, neboť jiné hry nejsou v těchto zemích populární, protože zde není příliš velká různorodost hráčů v hraní her jako v evropských zemích a USA.

Vyšší počet uživatelů Steamu také naznačuje vyspělost země v herním průmyslu a v současné je nedílnou součástí průmyslu e-sport. Všechny země zmíněné názvem v grafu mají několik profesionálních týmů a organizací soutěžících celosvětově. Jedinou zemí, která zde chybí je Jižní Korea, v celkovém zastoupení je Jižní Korea třetí v pořadí nejvýdělečnějších hráčů a počtu hráčů, pokud by se braly jiné platformy a videohry³⁹, ale výše zmíněný graf je zaměřen jen na Steam. [53]

³⁹ League of Legends od Riot Games a Starcraft II od Blizzard Entertainment.

Nejpopulárnější Steam hry

Pořadí	Název herního titulu	Online hráčů	Denní maximum hráčů	Odehraných hodin
1	Dota 2	898 071	1 141 191	465 890 274
2	Counter-Strike: Global Offensive	557 090	661 985	238 291 028
3	Sid Meier's Civilization VI	127 779	131 768	1 510 298
4	Team Fortress 2	61 173	68 825	31 587 612
5	Grand Theft Auto V	51 890	79 175	28 328 837
6	Rocket League	42 496	59 526	23 135 314
7	Paladins	42 374	56 034	20 426 936
8	Sid Meier's Civilization V	39 577	72 026	29 862 631
9	Rust	35 516	48 435	17 905 293
10	Garry's Mod	35 038	51 015	18 271 428
11	ARK: Survival Evolved	33 355	61 560	24 552 627
12	Football Manager 2016	29 513	55 882	20 709 124
13	Unturned	28 882	48 001	16 112 108
14	The Elder Scrolls V: Skyrim	27 152	39 759	15 711 987
15	Warframe	26 518	34 007	15 262 123
16	Arma 3	25 415	41 168	15 002 434
17	PAYDAY 2	24 951	41 053	8 780 323
18	Fallout 4	23 434	37 097	14 809 955
19	Counter-Strike	20 071	23 413	9 334 694
20	H1Z1: King of the Kill	17 842	26 869	10 957 218
21	Euro Truck Simulator 2	16 236	20 451	6 694 685
22	Terraria	16 009	23 776	9 449 209
23	Dead by Daylight	15 494	22 799	8 565 415
24	War Thunder	14 123	24 737	8 042 381
25	Football Manager 2017	14 065	16 892	668 067
Celkem steam uživatelů online		11 307 573		
Uživatelé ve hře		3 088 612		

Tabulka 2 Celosvětová statistika Steam ke dni 21. 10. 2016 v 18h 51min [67], zpracoval: Autor

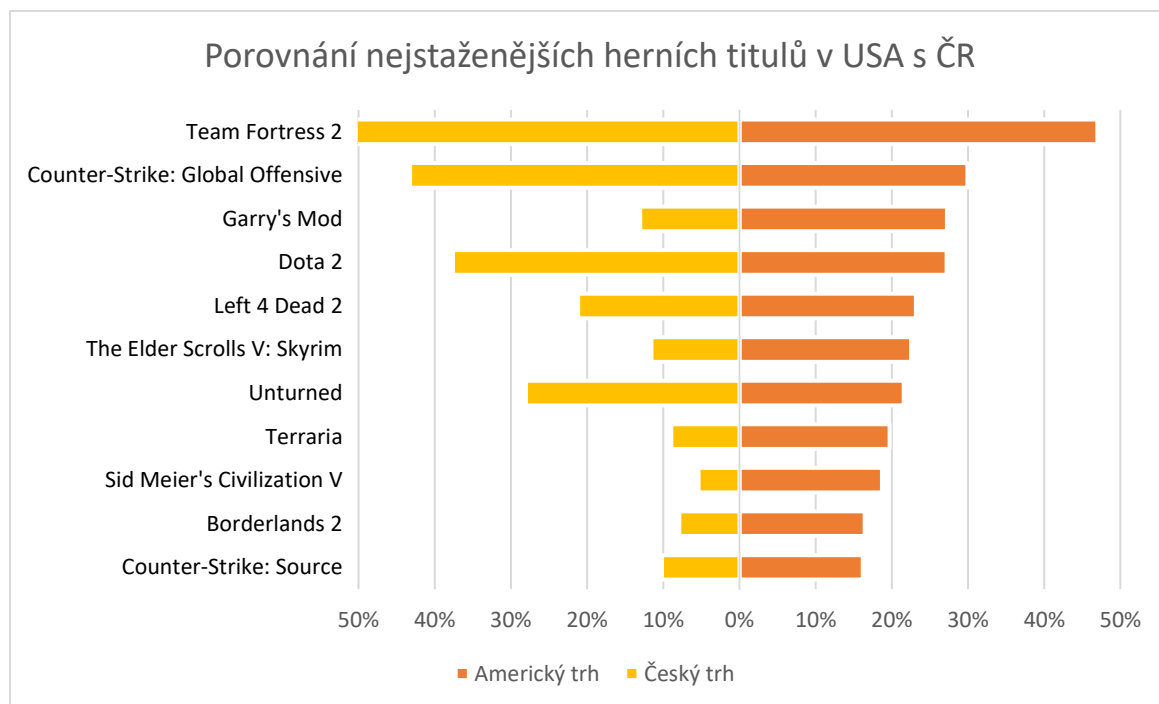
Dota 2 je již několik let nejpopulárnější a také nejaktualizovanější hrou na Steamu, přičemž důvodem je, že vlastníkem hry je v současné době Valve⁴⁰, tedy stejný vlastník jako v případě Steamu. Hra je dále známá v oblasti e-sportu a profesionálních hráčů v této hře.

Následuje další hra od Valve, tentokrát FPS hra CS:GO. Důvodem popularity je to, že je úplně totožná s první hrou Dota 2, pouze s rozdílem v počtu hráčů, neboť hru CS:GO je nutno koupit, patří do kategorie B2P, za dnešní cenu 13,99 eur.

⁴⁰ Kdysi existovala hra DotA (Defense of the Ancients), která byla jen herní modifikací hry Warcraftu, poté však byl vývoj zakoupen společností Valve. Dále se vyvíjí od roku 2012 pod názvem DotA.2.

Za zmínku stojí také v pořadí třetí hra Sid Meier's Civilizations VI, která se na první pohled liší od všech ostatních her v počtu odehraných hodin, což naznačuje novou hru na platformě. V tabulce popularity je i české zastoupení, Arma 3 vyvíjená vývojářským studiem Bohemia Interactive Studio se sídlem v Mníšku pod Brdy. [68]

7.2.2 Americký a český trh



Obrázek 15 Herní rozložení v USA s ČR ke dni 21. 10. 2016 [66], zpracoval Autor

K porovnání s trhem v České republice jsem si zvolil největší trh na Steamu, jímž je trh americký. Byly vybrány nejstahovanější herní tituly v USA a k nim byla zjištěna česká data pro porovnání. Procenta naznačují, kolik uživatelů Steamů jednotlivých zemí má staženou danou hru k celkovému počtu uživatelů Steamu.

Na prvních dvou místech jsou FPS hry Team Fortress 2 a CS:GO, první ze zmíněných patří do kategorie F2P her s možností dokoupení virtuálních věcí a rozšíření. Mezi další významné hry obou trhů patří nejhranější hra na platformě, Dota 2 a poté Unturned. Hlavním parametrem vysokého stažení těchto her je F2P kategorizace.

Další zajímavý pohled je na zbylé hry, které jsou oproti českému trhu na americkém trhu nadměrně stahované. Řeč je o hrách Garry's Mod, The Elder Scrolls V: Skyrim a Sid Meier's Civilization V a další v pořadí. Všechny tyto hry patří do kategorie B2P, je tedy potřeba koupit je za určitou cenu. Lze konstatovat, že český trh více preferuje hry F2P a má menší rozmanitost stažených her.

7.3 SWOT analýza

Silné stránky	Slabé stránky
• Přes 125 mil. registrovaných uživatelů • Denní aktivita 8-12 mil. uživatelů online • Přes 10 000 her poskytnutých pro operační systémy Windows, OS X a Linux [69] • Jednoduchost komunikace mezi přáteli • Přenos koupených her na jiné počítače • Možnosti offline i online hraní • Velký výběr her a herních aplikací • Vlastní VR přístroj • Steam klient přeložen do 28 jazyků	• Ne všechny hry jsou dostupné pro jednotlivé operační systémy • Stahování nových her vyžaduje hodně místa na pevném disku • Zatížení počítače hrami • K některým hrám je potřeba dokoupit rozšíření • Nevyžádané reklamy v online hrách • Nestabilní internetové připojení na Steam serverech
Příležitosti	Hrozby
• Růst herního průmyslu • Poskytování mobilních aplikací a her • Vyšší zájem o video hry u žen • Rozšíření VR do jiných her • Možnost rozšíření do jiných sfér průmyslu (hudební, filmové atd.) • Více herních serverů po celém světě	• Lepší distributor digitálních klíčů a her • Úbytek hráčů z důvodů Steam výběru her • Externí poskytovatelé jednotlivých her • Nefungující přihlašování • DDoS útoky na herní servery, vznik výpadku serveru • Bezpečnostní rizika přihlašování na účet • Stížnosti a soudní řízení proti společnosti Valve

Tabulka 3 Swot analýza Steamu, zdroj: Autor

Pro účel této práce je nejdůležitější sekce „Hrozby“, kterou se práce bude dále zabývat. Steam má několik potíží s online útočníky a zloději, protože díky své popularitě na trhu přináší mnoho peněz do systému.

8 ÚTOKY NA STEAMU

V rámci této kapitoly jsem vybral osm typů útoků, se kterými se lze na Steamu setkat. Všechny stručně zanalyzuji, názorně vysvětlím princip útoků a jejich výskyt na této platformě z pohledu útočníka. Útoky jsou kategorií herního scamu, u kterého je využita falešná identita, tedy phishing.

Cílem této kapitoly je vyhodnocení nejnebezpečnějších útoků na Steamu z hlediska úspěšnosti provedení útoku na nového uživatele platformy a zjistit, zda jsou phishingové útoky nebezpečné.

8.1 *Vybrané útoky*

Existuje mnoho forem útoků a krádeží v online hrách, v tomto případě jsem vybral útoky na základě vlastních zkušeností z hraní online her zejména na počítačové platformě Steam a jejích her.

1. Phishingové odkazy při obchodování;
2. Rychlé prohazování při obchodu;
3. Programy ke zlepšení hry;
4. Phishingový e-mail od společnosti;
5. SSFN kód;
6. Zneužití jména middlemana;
7. Paypal chargeback;
8. In-game scam;

8.2 *Kritéria vyhodnocení nebezpečnosti útoků*

Kritériem vyhodnocení jednotlivých útoků je osm níže zvolených parametrů, ke kterým je vždy uvedena otázka k analýze útoků. K jednotlivému parametru je dále přidána konkrétní váha, která určuje míru nebezpečnosti parametru, a k finálnímu vyhodnocení nebezpečnosti útoku jsou přiděleny body s rozptylem 1-3, kdy vyšší bodové označení znamená vyšší míru úspěšnosti provedení útoku.

- Relevance se Steamem;
- Sofistikovanost;
- Délka provedení;
- Důvěryhodnost;
- Rozsah využití;
- Konkrétní cíl;

- Škody;
- Opakovatelnost.

Relevance se Steamem

Každý z vybraných útoků je spojen se Steamem jako zprostředkovatelem, avšak některé útoky lze provést jinou herní platformou nebo mimo herní zprostředkovatele. Tento parametr slouží jako míra návaznosti Steamu na vybrané útoky. V tomto případě má 3 body „Nutná potřeba Steamu“, neboť se měří nebezpečnost vůči uživatelům Steamu. Pokud by se jednalo o obecné uživatele, prohodila by se tato položkou s poslední ohodnocenou bodově 1.

Body	3	2	1
Popis	Nutná potřeba Steamu	Možnost útoku i na jiných herních platformách	Útok je realizován i mimo herní průmysl

Otázka: Je potřeba Steam k provedení útoku a do jaké míry?

Váha: 8 %

Sofistikovanost

Kyberútoky jsou součástí informačních technologií a nedílnou součástí je programování. Čím je vyšší náročnost a sofistikovanost útoku, tím je také větší šance na jeho úspěšnost. Významnou roli hraje časová příprava útoku, která je součástí tohoto parametru.

Body	3	2	1
Popis	Velmi náročné na technické zpracování a programování	Základní až pokročilejší znalost programování	Není potřeba programování

Otázka: Jak dlouhé a náročné je naprogramovat tento útok?

Váha: 5 %

Délka provedení

Dalším parametrem hodnocení je délka provedení, která se od jednotlivých útoků liší. K některým je potřeba vykonat určité akce, aby se dospělo k závěru, tedy krádeži.

Body	3	2	1
Popis	Do pár hodin či minut	Během pár dnů	Týdny až měsíce

Otázka: Jak dlouho bude trvat, než se oběť chytne?

Váha: 10 %

Důvěryhodnost

Úspěšnost útoků je nejvíce závislá na parametru důvěryhodnost útoku, neboť prvním krokem všech útoků je nalákat oběť na infikovaný soubor či webovou stránku, které byly vytvořeny za účelem krádeže osobních informací, virtuálních věcí a peněz.

Body	3	2	1
Popis	Velmi důvěryhodné	Malé pochybnosti	Známý útok, nedůvěryhodný

Otázka: Jak moc je útok důvěryhodný?

Váha: 40 %

Rozsah výskytu

Šíření útoků je dalším důležitým parametrem, který zvyšuje úspěšnost daného útoku. Jednotlivý útok má vyšší množství rozeslání.

Body	3	2	1
Popis	Útok je realizován i mimo herní průmysl	Možnost útoku na jiných platformách	Útok je určen jen pro jednu oblast her

Otázka: Kolik potenciálních obětí lze nalákat?

Váha: 10 %

Konkrétnost cíle

Podle tohoto parametru se určí, zda je útok zaměřen na konkrétní herní komunitu či jednotlivce.

Body	3	2	1
Popis	Výběr je náhodný	Zaměřeno na lidi se stejnými vlastnostmi a zálibami	Specifický na konkrétní skupinu/osobu

Otázka: Je útok jen na určitou skupinu osob?

Váha: 5 %

Škody

K provedeným útokům vždy existují určité škody, rozsah jednotlivých útoků je ovlivněn dle napadených údajů a jejich zneužití.

Body	3	2	1
Popis	Ztráta osobních údajů a další zneužití	Ztráta cenných virtuálních věcí a účtů	Ztráta virtuálních peněz a věcí

Otázka: Jak veliké škody přinese útok?

Váha: 10 %

Opakovatelnost

Poslední parametr zjišťuje, zda je možné opakovat stejný útok na konkrétní oběť, která podobnou situaci již zažila.

Body	3	2	1
Popis	Útok již nese rizika, se kterými oběť počítá	Pochybení ze strany oběti	Oběť se znovu nenaláká

Otázka: Lze útok opakovat?

Váha: 12 %

8.3 Metodika vyhodnocení útoku

Jednotlivé útoky jsou podrobeny stručnému popisu⁴¹ od začátku až do konečného provedení. V popisu útoku je obsažen nejprve název a cíl útoku, dále jeho podmínky a nástroje provedení a obsah zprávy k nalákání oběti. Na závěr jsou vyhodnoceny parametry dle zkušeností autora se situacemi. Všechny útoky jsou umístěny v přílohách práce, viz kapitola 14 Přílohy.

Míra nebezpečí útoku informuje nového uživatele Steamu o tom, jak často se s daným útokem setká, jaká je potenciální úspěšnost s poměrem škod a je vypočítán pomocí váženého průměru s procentuálním vyhodnocením zaokrouhleným na 2 desetinná místa.

$$\text{Vzorec: } \bar{\mathcal{X}} = \frac{\sum_{i=1}^{k=n} v_i \cdot p_i}{m} * 100$$

n = počet parametrů útoků (8), v_i = hodnota váhy parametru, p_i = bodové ohodnocení parametru, m – maximální hodnota celkového vyhodnocení (3)

⁴¹ Z hlediska náročnosti detailního provedení na programování některých útoků jsem zvolil jen krátký popis principu útoku z hlediska útočníka.

8.4 Vyhodnocení všech útoků

Název útoku	Míra nebezpečnosti (v %)	Pořadí
Phishingové odkazy při obchodování	90.00	1.
Rychlé prohazování při obchodu	72.33	5.
Programy ke zlepšení hry	69.00	6.
Phishingový e-mail od společnosti	84.67	2.
SSFN kód	75.33	4.
Zneužití jména middlemana	56.67	7.
Paypal chargeback	84.00	3.
In-game scam	50.67	8.

Tabulka 4 Vyhodnocení míry nebezpečnosti útoků, zdroj: Autor

8.5 Shrnutí

Nejnebezpečnějším útokem na Steamu jsou oba útoky s phishem, neboť tyto útoky jsou nebezpečné zejména z hlediska rozsáhlosti, jednoduchosti a rychlosti provedení. Poté velice záleží na schopnostech útočníka nalákat oběť, od kterých se pak odvíjí míra důvěryhodnosti. Zároveň v současnosti patří mezi nejdiskutovanější téma z hlediska online krádeží na Steamu. [70]

Míra nebezpečnosti spočívala zejména v uskutečnění útoku, který byl zahrnut v parametru „Důvěryhodnost“ s nejvyšší vahou 40 %. Nejvyšší důvěryhodnost s hodnotou 3 byly oba phishingové útoky a také útok s Paypalem, který je v pořadí třetí nejnebezpečnější. I když se útok zaměřuje zejména na herní účty a virtuální věci, útok tímto způsobem je téměř zaručeně úspěšný a návratnost ztracených položek je nulová. Důvodem nenávratnosti je, že Paypal při obchodech s virtuálním zbožím má velice složitý proces hlídání obchodu, neboť finální obchod a podmínky jsou zrealizovány mezi dohodnutými stranami.

Za připomenutí stojí také útok SSFN kódem, který je závažný hlavně kvůli škodám, jeho parametr měl ze všech útoků nejvyšší bodový zisk. Jako jediný ohrožoval platební údaje uživatele a ztracení kompletního účtu na Steamu. SSFN kód je součástí SteamGuard viz kapitola 9.4.

Zbýlé útoky byly méně nebezpečné, neboť byly specifické tím, že se zaměřovaly na určité skupiny lidí, kteří již nesou nějaké herní zkušenosti z předešlých her a znají obdobné situace mimo videohry. Realizace útoků a jejich dopady jsou velmi nízké.

8.5.1 Cíl útoků

Cílem všech útoků bylo získat od oběti přihlašovací údaje či herní věci a peněz. U útoku se SSFN kódem je největší riziko krádeže i platebních údajů, které si oběť mohla uložit, neboť útočník tímto způsobem získá veškerou kontrolu nad ukradeným účtem. Celkově byly útoky již tematicky směřovány na herní platformu Steam, ale kromě útoku se SSFN kódem by se mohly využít všechny útoky v jiných herních a mimo herních prostředích.

8.5.2 Zjištění informací oběti

Za prvé je potřeba zjistit, kde se útok provede. Steam umožňuje několik cest, jak se k tomu propracovat, díky celosvětovému ohlasu své platformy. Jestliže útok bude směřován náhodně a výběr obětí také, lze využít jen nějaká herní fóra, která jsou méně významná a zabezpečená. V takových místech jsou však útoky méně úspěšné, neboť zkušenější hráč rozpozná kvalitu webové stránky a její možnosti, cílem jsou proto nezkušení hráči. Příkladem mohou být služby k vylepšení herních postav, účtů nebo získání nových herních věcí.

Další fází výběru potenciálních obětí je již na větších herních portálech, u kterých je potřeba autentizace Steam. Tyto portály jsou bezpečnější, jelikož disponují vyšším počtem uživatelů, kteří formou diskuzních fór upozorňují na možná rizika phishingových stránek a phisherů. Tito nevídaní uživatelé jsou rychle zneškodněni a zabanováni z komunity. Podmínkou však je zjistit, kdo je zlodějem. Nalezení zloděje lze až po pokusu o krádež, a to až v případě vydařeném, či nevydařeném.

V těchto případech je zvolena metoda, které jsou z hlediska jednoduchosti nejvíce pravděpodobné, jde o společné přátele. Steam umožňuje uživatelům prohlédnout si seznam přátel konkrétních osob, zda mají nastavený veřejný profil, pak přidá jednu z přátel oběti. Oběť je nalákána na základě doporučení přidaného společného přítele, který o tom ve skutečnosti nemá tušení. Pro úspěšný útok je zapotřebí nevědomosti a nezkušenosti oběti, tedy to, aby se nechala nalákat. Záleží také na komunikační schopnosti útočníka.

8.5.3 Návnada

Útoky, které získávaly přihlašovací údaje přes webový odkaz, bylo nutné vytvořit vlastní phishingovou webovou stránku. Prvním krokem je zvolení serveru pro naši webovou stránku, kterou však musím nejprve vytvořit. Jako původní stránku je zvolena logovací stránka <https://steamcommunity.com/login/>, ze které bylo potřeba zkopírovat vzhled a úroveň sofistikovanosti se pak pomocí programování v jednotlivých funkcích liší.⁴²

⁴² Které nebyly z hlediska náročnosti a rozsáhlosti zahrnuty v této práci.

8.5.4 Rozeslání útoku

K rozeslání útoků posloužil Steam obchod a chat, útok byl také možný pomocí herních prostředí, která jsou zabudována v online hrách. Výhodou útoků prostřednictvím online her byla vyšší úroveň soukromí útočníka, neboť údaje, které byly zadávány v online hrách, nebyly dostatečně informující. Informace v hrách se získávají nejčastěji pouze přímým kontaktem a osobním sdělením od uživatele.

8.5.5 Zneužití získaných informací

Prodej, krádež a další obchodování se získanými věcmi je nejběžnější praktikou ukradených účtů. Útočník se rovněž může pokusit o zneužití těchto přihlašovacích údajů i na sociálních médiích, Google a iCloud účtech, které jsou v dnešní době součástí a nutností téměř všech uživatelů digitálního světa.

8.5.6 Zahlazení stop

Útočník má mnoho možností schovat se před oběťmi, tím se vyhnout vrácení ukradeného a zaplacení škod. K nejčastějším metodám patří vytvoření falešného účtu na Steamu za účelem konkrétního útoku na konkrétní osobu, poté tento účet smazat. Útok lze vylepšit tím, že útočník využije kradený účet, který zpravidla není nový. Účet může vlastnit několik her s mnoha odehranými hodinami, dále obsahovat pozitivní recenze od jiných uživatelů, a proto může evokovat vyšší důvěryhodnost osoby. Po útoku existuje možnost jako u předešlé situace, a to smazání, zablokování a přejmenování účtu nebo ponechání účtu po nějakou dobu neaktivního s cílem dalšího zneužití.

Ve virtuálních hrách je situace jednodušší, neboť administrativa hry již nespadá do rukou Steamu⁴³ a po nahlášení útočníků dojde maximálně k zablokování na danou hru, ne na celou Steam platformu.⁴⁴

⁴³ Výjimky jen u Steamem autorizovaných her, jako je například hra Dota 2 a Counter Strike: Global offensive

⁴⁴ Avšak záleží na rozsáhlosti a závažnosti škod útoku.

9 ZABEZPEČENÍ NA STEAMU

Steam patří mezi jednu z největších platforem distribuce digitálních her, a proto je k dispozici velká škála bezpečnostních opatření. Nejčastějšími místy krádeže jsou herní fóra, portály, herní služby, zejména pak trh elektronických věcí, které nejsou certifikovány partnery Steam, tudíž je zde vyšší výskyt úspěšných krádeží. Závěr této kapitoly obsahuje bezpečnostní vyhodnocení předešlých útoků za použití jednotlivých bezpečnostních nástrojů a prvků.

- Reakce na phishing;
- Podmínky využívání služeb;
- E-mailové zabezpečení;
- Mobilní zabezpečení;
- SteamGuard.

9.1 Obecné návyky

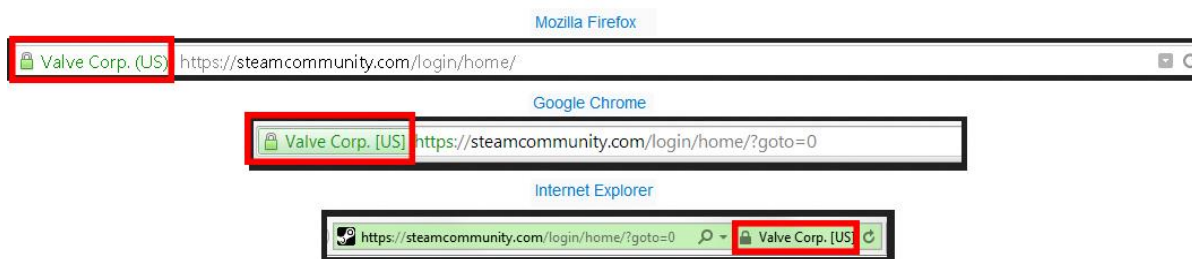
Bezpečnost Steam účtu je jedním z nejvíce nahlížených témat platformy s téměř 200 milióny celkových zhlédnutí. Steam podpora sděluje všem hráčům a uživatelům obecné, ale výstižné pravidlo: „*Nikdy nikomu nesdílejte heslo a nikdy neklikejte na odkazy nedůvěryhodných osob!*“ [70]

Dalšími sděleními a upozorněními jsou phishingové stránky, na kterých jsou přeházená nebo upravená písmenka původního odkazu, ale vzhled je totožný. Valve je asociována s těmito doménami. (Obrázek 16)

- <https://steamcommunity.com>
- <https://steampowered.com>
- <https://store.steampowered.com>
- <https://support.steampowered.com>

Obrázek 16 Původní domény [77]

Steam vyzývá uživatele, aby si v prohlížeči ověřili skutečnou webovou stránku dle certifikátu obsahujícího Valve Corp. (Obrázek 17)



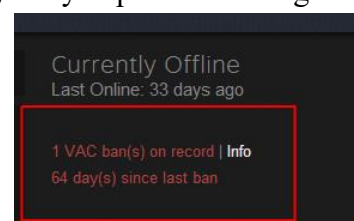
Obrázek 17 Certifikáty v jednotlivých prohlížečích zdroj: Autor

Celkové shrnutí k bezpečnému zabezpečení ze strany uživatele je následovné:

- Zvolení silného hesla, tj. využití číselných i nečíselných znaků s různou velikostí písma.
- Unikátní hesla neasociovaná s jinými službami a platformami.
- Pravidelné kontroly počítače pomocí antivirů.
- Vyhnout se přihlášení na nezabezpečené počítače (internetové kavárny).
- Vždy se odhlásit z cizích počítačů. [70]
- Obchodovat jen s ověřenými uživateli.

Platforma umožňuje hráčům ověřit si důvěryhodnost jakéhokoliv účtu pomocí VAC (Valve's Anti-Cheat) upozornění na profilu každého uživatele, který nepoctivě či vulgárně reagoval v předchozích situacích. (Obrázek 18)

Platforma také umožňuje několik opatření účtů, která nejsou povinná, ale doporučená. Níže jsou podrobněji popsána jednotlivá zabezpečení.



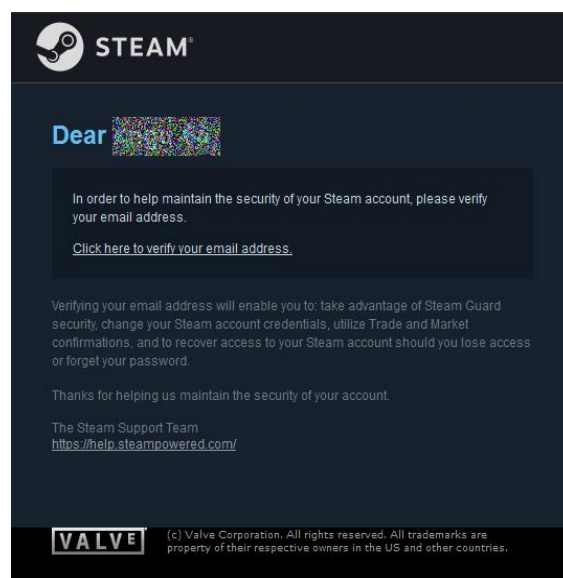
Obrázek 18 Účet s VAC upozorněním, zdroj: Autor

9.2 E-mailové zabezpečení

E-mailové zabezpečení je prvním krokem k úspěšnému zabezpečení na Steamu. Po vytvoření Steam účtu je zapotřebí verifikovat e-mail, na kterém byl účet vytvořen. (Obrázek 19) E-mail slouží jako prostředek k informování o případných změnách na účtu. Dále e-mail slouží k informování o veškerých transakcích provedených na Steamu.

9.3 SMS zabezpečení

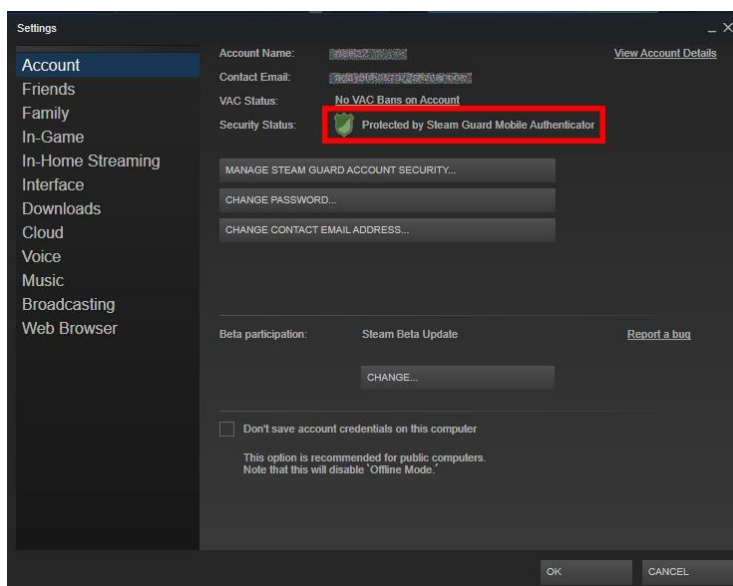
Zabezpečení pomocí mobilního čísla je další formou opatření a slouží k rozšíření možností při zapomenutí hesla na účet i na e-mail. Funkcí mobilního zabezpečení je, že při jakémkoliv autentizaci účtu je na mobil poslán unikátní kód prostřednictvím SMS zpráv. V současné době je tento způsob nahrazen mobilní aplikací SteamGuard, která umožňuje nejvyšší zabezpečení z technického hlediska.



Obrázek 19 Odkaz v e-mailu k verifikaci, zdroj: Autor

9.4 SteamGuard

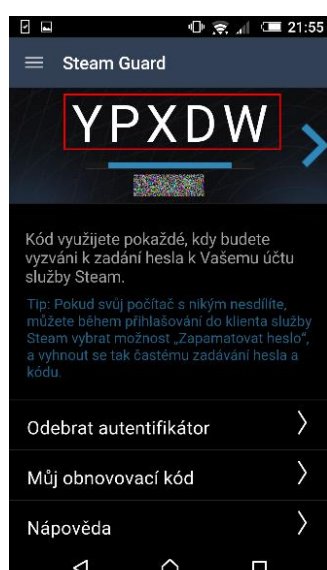
SteamGuard je dvoufaktorové opatření proti zlodějům a nezvaným hostům účtu. SteamGuard je součástí mobilní verze Steam a je zdarma dostupné na všech platformách. (Obrázek 20) Obsahuje autentizaci pomocí unikátních kódů, které však oproti mobilnímu zabezpečení mají časový limit na použití, který činí 30s, pak je znovu obnoven na mobilním zařízení. (Obrázek 21) Tento kód je vždy generován při novém přihlášení, úpravách účtu či transakci. (Obrázek 22)



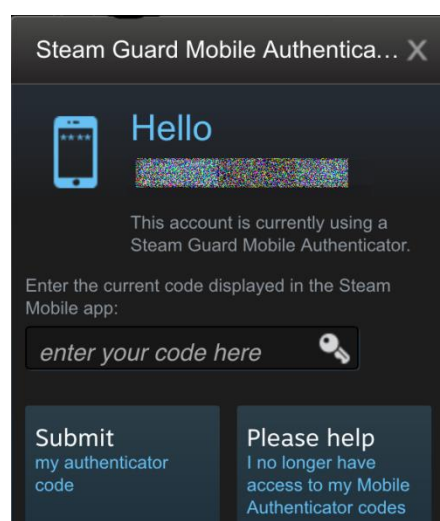
Obrázek 20 Úspěšná validace SteamGuardu, zdroj: Autor

Nevýhodou této služby je, že v případě ztracení mobilního telefonu je doporučeno kontaktovat mobilního operátora a požádat o zaslání stejného čísla, v případě komplikací je zapotřebí doložit důkaz totožnosti pomocí údajů o transakcích nákupů, což je velmi náročný proces [70]

Autentizační kód SteamGuardu lze obejít pomocí SSFN souboru umístěného ve složce Steam, která obsahuje kód k obcházení této autentizace.



Obrázek 21 Vygenerovaný kód na mobilu, zdroj: Autor



Obrázek 22 Výzva zadání kódu, zdroj: Autor

9.5 Závěrečné bezpečnostní vyhodnocení k vybraným útokům

Název útoku	Obecné návyky	E-mailové zabezpečení	SteamGuard
Phishingové odkazy při obchodování	✓	✓	✓
Rychlé prohazování při obchodu	✗	✗	✗
Programy ke zlepšení hry	✗	✓	✓
Phishingový e-mail od společnosti	✓	✓	✓
SSFN kód	✓	✗	✗
Zneužití jména middlemana	✓	✓	✗
Paypal chargeback	✗	✗	✗
In-game scam	✓	✗	✗

Tabulka 5 Bezpečnostní vyhodnocení útoků, zdroj: Autor

Opatření na technické útoky je SteamGuardem od Steamu velice účinné proti phishingovým útokům, které zajistí 100% ochranu, avšak u útoků, které jsou zaměřeny na virtuální věci a peníze, se nedá toto opatření využít. Dále existuje e-mailové zabezpečení, které jen informuje a upozorňuje na nebezpečné a neověřené webové aktivity účtu.

Poslední opatření z obecných návyků je ze všech nejspolehlivější z hlediska zabránění úspěšného útoku, neboť uživatelé, kteří se s kyberútoky již dříve setkali a mají vyšší znalost o principu jednotlivých útoků a jejich zaměření, se ve většině případů zranitelnosti vyhnou.

Útok Paypalem byl ze všech vybraných útoků nejnebezpečnější z hlediska zabezpečení. Jak již bylo dříve v práci zmíněno, metoda útoku spočívá v důvěře obou obchodujících stran a jediným opatřením je dostatek informovanosti o dané osobě ve formě recenze důvěryhodnosti.

Jeden ze dvou útoků, který obcházela obecné návyky, byl útok „Programy ke zlepšení hry“. Oběť v této situaci již počítá s riziky těchto programů, které jsou ve většině případů nelegální. V mnoha případech se lze proti nim technicky zabezpečit, ale k využívání těchto služeb/aplikací je většinou potřeba vypnout všechna technická bezpečnostní opatření.

10 ZÁVĚR

Jedním ze dvou cílů práce bylo poskytnout základní přehled o bezpečnostních rizicích při online obchodování obecně a v herním průmyslu ve formě phishingu a scamů. V teoretické části jsem nejdříve vysvětlil základní pojmy a postupy k problematice phishingu. V následující kapitole jsem detailně popsal herní průmysl z historického vývoje po současné trendy v této oblasti. Dále jsem uvedl stručný popis jednotlivých herních žánrů na trhu herního průmyslu a poté jsem popsal bezpečnostní rizika v herním průmyslu ve formě phishingu a scamu v běžném a herním phishingem. Teoretická část práce je zakončena kapitolami o druzích útoků phishingu a o možnosti ochrany proti phishingu z obecného hlediska. Za nejzajímavější část považuji kapitolu E-sports, což je fenomén, který je v současné době velmi rychle se rozvíjející z hlediska sledovanosti, z finanční stránky ve formě investic a jako poslední, z možnosti realizace plnohodnotného kariérního rozvoje v e-sportu.

K dosažení druhého cíle, kterým bylo poskytnutí budoucím a stávajícím uživatelům platformy Steam přehled o běžných phishingových útocích a protiopatřeních, jsem v analytické části stručně popsal herní platformu Steam a její funkce, ve kterém následovalo porovnání amerického a českého trhu platformy, zakončené SWOT analýzou. V praktické části jsem si vybral osm útoků na Steamu, se kterými jsem se setkal, vyhodnotil jsem je dle vlastních zkušeností. V závěru praktické části práce jsem poskytl přehled o bezpečnostních zabezpečeních společnosti Steam, poté jsem tato opatření aplikoval na vybrané útoky.

Potvrdilo se, že mezi nejrizikovější útoky patří útoky pomocí phishe, ale s patřičným technickým opatřením od Steamu se lze proti těmto útokům dobře zabezpečit. Ačkoliv bylo po analýze zjištěno také několik útoků, proti kterým se nelze zabezpečit pomocí prostředky Steamu, tak jedinou bezpečnou metodou užívání platformy je ohleduplnost a dostatečná informovanost ze strany uživatele, což bývá vždy největším bezpečnostním problém ve všech oblastech kyberprostoru.

Oba výše zmíněné cíle byly naplněny a za hlavní přínos práce považuji, že může posloužit jako dílčí návod k bezpečnému obchodování v herním průmyslu, zejména pak v online hrách a herních platformách, které jsou v dnešní době cílené zejména na „nováčky“ v oblasti her, kteří dosud neznají metody online okrádání pomocí videoher. V práci jsem stručně vysvětlil základní herní pojmy, se kterými se lze dále běžně setkat i mimo her.

Práce může sloužit k dalšímu zpracování, a to buď naprogramováním těchto útoků a provedením jejich testování na uživatelích s náležitými protiopatřeními, nebo hlubší analýzou herního průmyslu z finančního a technologického hlediska jednotlivých žánrů a platforem videoher.

11 TERMINOLOGICKÝ SLOVNÍK

Termín	Zkratka	Význam [zdroj]
Phishing		Počítačový útok, který cílí na okrádání osobních a přihlašovacích údajů, pomocí podobně vypadající webové stránky. [zdroj Autor]
Pharming		Specifičtější útok phishingu s cílem okrádání konkrétní osoby či společnosti. [zdroj Autor]
Phish		Útok phishingu. [zdroj Autor]
Phisher		Útočník phishingu [zdroj Autor]
Herní scam		Oproti běžnému scamu je herní specifický v prostředí, kterým je virtuální svět her. [zdroj Autor]
Malicious software	Malware	Škodlivý program sbírající citlivé údaje počítače a získávající přístupy na soukromé počítačové systémy. [15]
3D hry		Trojrozměrné rozhraní virtuálního světa počítačové hry. Možnost rotace pohledu hráče. [zdroj Autor]
2D hry		Dvojrozměrné rozhraní virtuálního světa počítačové hry s jednou perspektivou hráče. [zdroj Autor]
Facebook		Mezinárodní sociální síť s více než miliardou aktivních uživatelů. [zdroj Autor]
Smartphone		Mobilní telefon, který využívá pokročilý mobilní operační systém a aplikační rozhraní, jež umožní instalaci nebo úpravy programů, zvaný chytrý telefon. [71]
Virtuální realita	VR	Technologie, která umožní uživateli interagovat s počítačově vygenerovaným skutečným světem. [zdroj Autor]
Massively Online Role Playing Game	MMORPG	Rozsáhlá online hra s jednou ústřední postavou s cílem vytrénovat na určité herní úrovni a poté splnit herní mise. Hra je hrána s více lidmi, někdy i s tisíci lidmi zároveň. [zdroj Autor]
Herní streaming		Natáčení sebe sama při hraní her či jiných herních aktivitách. Nejznámější platformou je Twitch.tv. [zdroj Autor]

Online hry		Hry hrané prostřednictvím internetu s možnostmi interakcí s jinými hráči. (multiplayer hry) [zdroj Autor]
Offline hry		Hry bez přístupu internetu a hrané bez přítomnosti jiných hráčů. Většinou se jedná o single player hry (hry s jednou osobou). [zdroj Autor]
Steam		Multifunkční platforma distribuující zejména herní tituly a jiné aplikace. [zdroj Autor]
Steam účet		Účet platformy Steam, ze kterého lze pustit jednotlivé aplikace a hry. [zdroj Autor]
In-game prostředí		Herní svět v online a offline hrách. [zdroj Autor]
Herní ban		Ban, který je udělen hráči za nevhodné a nebezpečné chování v hrách. [zdroj Autor]
Herní účet		Účet, který obsahuje herní postavu v online hře. [zdroj Autor]
Middleman		Nestranná osoba mezi dvěma obchodujícími stranami, která zajišťuje a dohlíží na bezpečné provedení obchodu. [zdroj Autor]

12 SEZNAM POUŽITÉ LITERATURY

- [1] **Lance, James.** *Phishing bez záhad.* [překl.] Miroslav Moudrý. Praha : Grada, 2007. str. 281. ISBN 9788024717661.
- [2] **MVČR.** *Základní definice, vztahující se k tématu kybernetické bezpečnosti.* Praha, Česká republika : Ministerstvo vnitra ČR, 2009.
- [3] **Phneah, Ellyne.** Anticipating threats ineffective in enhancing security. *ZDnet*. [Online] 19. 11 2012. [Citace: 4. 10 2016.] <http://www.zdnet.com/article/anticipating-threats-ineffective-in-enhancing-security/>.
- [4] **Baker, Liana B.** Factbox: A look at the \$65 billion video games industry. *Reuters*. [Online] 6. 6 2011. [Citace: 6. 10 2016.] <http://uk.reuters.com/article/us-videogames-factbox-idUKTRE75552I20110606>.
- [5] **Neagu, Aurelian a Chipurici, Christina.** Top Online Scams Used by Cyber Criminals to Trick You [Updated]. *Heimdall Security*. [Online] 5 2016. [Citace: 11. 10 2016.] <https://heimdalsecurity.com/blog/top-online-scams/>.
- [6] **Computing.** Malware. *Computing*. 10. 3 2006, str. 49.
- [7] **Meleney, Lisa.** IT Services Insights: Dyre Malware Has Stolen Over \$1 Billion: Is Your Company's Sensitive Data at Risk? *Bay Computing*. [Online] 18. 11 2015. [Citace: 13. 10 2016.] <http://blog.baymcp.com/blog/dyre-malware-has-stolen-over-1-billion-is-your-companys-sensitive-data-at-risk>.
- [8] **Bitto, Ondřej.** Rhybaření střídá pharming. *Lupa.cz*. [Online] 31. 3 2005. [Citace: 14. 10 2016.] <http://www.lupa.cz/clanky/rhybareni-strida-pharming/>.
- [9] **Phishing.org.** History of Phishing. *Phishing.org*. [Online] 2004. [Citace: 11. 10 2016.] <http://www.phishing.org/history-of-phishing/>.
- [10] **ScamVictimsUnited.** ScamVictimsUnited.com. *ScamVictimsUnited.com*. [Online] 13. 3 2003. [Citace: 13. 10 2016.] <http://scamvictimsunited.com/phpBB2/index.php>.
- [11] **ScamSurvivors.** ScamSurvivors.com. *ScamSurvivors.com*. [Online] 26. 3 2012. [Citace: 13. 10 2016.] <http://www.scamsurvivors.com/forum/>.
- [12] **ViRy.** Hoax & Phishing & Pharming. *ViRy.cz*. [Online] 25. 1 2000. [Citace: 13. 10 2016.] <http://forum.viry.cz/viewforum.php?f=6>.

- [13] **ALEC.** Anti-Phishing Act. *ALEC*. [Online] 1. 12 2012. [Citace: 14. 10 2016.]
<https://www.alec.org/model-policy/anti-phishing-act/>.
- [14] **Janousek, Michal.** *KYBERTERORISMUS: TERORISMUS INFORMACNÍ SPOLECNOSTI*. Brno, Czech Republic : University of Defence, 2006. Univerzita Obrany. Ustav Strategickych Studii. Obrana a Strategie. ISSN 12146463.
- [15] **Hák, Igor.** Moderní počítačové viry. [Online] 2005. [Citace: 16. 10 2016.]
<http://viry.cz/download/kniha.pdf>.
- [16] **De Prato, Giuditta, Feijóo, Claudio a Simon, Jean-Paul.** *Innovations in the Video Game Industry: Changing Global Markets*. Montpellier, France : Communications & Strategies, 2014. Communications & Strategies. ISSN 11578637.
- [17] **Zackariasson, Peter a Wilson, L. Timothy.** *The Video Game Industry: Formation, Present State and Future*. 1st edition. New York : Routledge, 2012. ISBN 9780203106495.
- [18] **Egenfeldt-Nielsen, Simon , Smith, Jonas Heide a Tosca, Susana Pajares .** *Understanding Video Games: The Essential Introduction*. 3rd edition. London : Routledge, 2016. str. 377. ISBN 9781138849822..
- [19] **MPAA.** Theatrical Market Statistics 2015. *Motion Picture Association of America*. [Online] 31. 12 2015. [Citace: 6. 10 2016.] http://www.mpa.org/wp-content/uploads/2016/04/MPAA-Theatrical-Market-Statistics-2015_Final.pdf.
- [20] **NewZoo.** Global Games Market Will Reach \$102.9 Billion in 2017. *NewZoo*. [Online] NewZoo, 14. 5 2014. [Citace: 6. 10 2016.] <https://newzoo.com/insights/articles/global-games-market-will-reach-102-9-billion-2017-2/>.
- [21] **Welch, Chris.** Amazon, not Google, is buying Twitch for \$970 million. *The Verge*. [Online] The Verge, 25. 8 2014. [Citace: 16. 10 2016.]
<http://www.theverge.com/2014/8/25/6066295/amazon-reportedly-buying-twitch-for-over-1-billion>.
- [22] **Statista.** Global revenues of the video game industry from 2003 to 2014 (in billion U.S. dollars) . *Statista*. [Online] 20. 12 2013. [Citace: 6. 10 2016.]
<https://www.statista.com/statistics/269744/global-revenues-of-the-video-game-industry-since-2003/>.

- [23] —. Value of the global video games market from 2011 to 2020 (in billion U.S. dollars). *Statista*. [Online] 15. 7 2015. [Citace: 6. 10 2016.]
<https://www.statista.com/statistics/246888/value-of-the-global-video-game-market/>.
- [24] **MPAA**. Theatrical Market Statistics 2011. *Motion Picture Association of America*. [Online] 31. 12 2010. [Citace: 6. 10 2016.]
https://wikileaks.org/sony/docs/03_03/Mktrsch/Market%20Research/MPAA%20Reports/2010/2010%20Theatrical%20Market%20Statistics.pdf.
- [25] **Ingham, Tim**. Global record industry income drops below \$15bn for first time in decades. *MusicBusinessWorldwide*. [Online] 14. 4 2015. [Citace: 6. 10 2016.]
<http://www.musicbusinessworldwide.com/global-record-industry-income-drops-below-15bn-for-first-time-in-history/>.
- [26] **Winter, David**. A.S.Douglas' 1952 Noughts and Crosses game:. *Pong-story*. [Online] 8. 7 2013. [Citace: 6. 10 2016.] <http://www.pong-story.com/1952.htm>.
- [27] **Poole, Steven**. *Trigger Happy: videogames and entertainment revolution*. 1st, New York, U.S. : Arcade, 2004. ISBN 1559705981.
- [28] **Cohen, Scott**. *Zap!: the rise and fall of Atari*. New York, U.S. : McGraw-Hill, 1984. ISBN 0070115435.
- [29] **Williams, Dmitri**. The History and Structure of the Video Game Industry. *Ninja Metrics*. [Online] 2014. [Citace: 7. 10 2016.] <http://cdn2.hubspot.net/hub/245562/file-632251833-pdf/v3/ebooks/gameHistory-eBook.pdf?t=1396479787000>.
- [30] **Nintendo**. Nintendo History. *Nintendo*. [Online] [Citace: 7. 10 2016.]
<https://www.nintendo.co.uk/Corporate/Nintendo-History/Nintendo-History-625945.html>.
- [31] **ESA**. Essential Facts about the computer and video game industry. *Entertainment Software Association*. [Online] 10. 5 2006. [Citace: 7. 10 2016.]
<https://library.princeton.edu/sites/default/files/2006.pdf>.
- [32] **Playstation**. Playstation Network. *Sony Playstation*. [Online] 2016. [Citace: 7. 10 2016.]
- [33] **Xbox**. Vítá vás Xbox Live. *Microsoft Xbox*. [Online] 2016. [Citace: 7. 10 2016.]
<http://www.xbox.com/cs-CZ/live?xr=shellnav>.

- [34] *Videogame industry overview (panel session): technology, markets, content, future.* **Veeder, Jane, a další.** New York : ACM, 1995. Proceedings of the 22nd annual conference on computer graphics and interactive techniques. Sv. SIGGRAPH '95, stránky 486-487. ISBN 9780897917018.
- [35] **Statista.** Number of World of Warcraft (WoW) subscribers from 1st quarter 2005 to 3rd quarter 2015 (in millions). *Statista*. [Online] 2015. [Citace: 8. 10 2016.] <https://www.statista.com/statistics/276601/number-of-world-of-warcraft-subscribers-by-quarter/>.
- [36] **Teamspeak.** About us. *Teamspeak Communication System*. [Online] 2001. [Citace: 7. 10 2016.] <http://www.teamspeak.com/about>.
- [37] **Bray, Hiawatha.** Players add verbal jabs to their arsenal. *Arts & Entertainment*. [Online] boston.com, 29. 10 2003. [Citace: 7. 10 2016.] http://archive.boston.com/ae/games/articles/2003/10/29/players_add_verbal_jabs_to_their_arsenal/.
- [38] **Croft, Charlene.** *A Brief History of Facebook*. 18. 12 2007.
- [39] **Ryan, Ninja.** The History and Structure of the Video Game Industry – Modern Era – Part 2. *Ninja Metrics*. [Online] Ninja Metrics, 24. 1 2014. [Citace: 7. 10 2016.] <https://www.ninjametrics.com/blog/the-history-and-structure-of-the-video-game-industry-modern-era-part-2/>.
- [40] **Juul, Jesper.** *A casual revolution: reinventing video games and their players*. London : MIT Press, 2010. ISBN 978-0-262-51739-3.
- [41] **NewZoo.** The Global Games Market Reaches \$99.6 Billion in 2016, Mobile Generating 37%. *NewZoo*. [Online] NewZoo, 21. 4 2016. [Citace: 8. 10 2016.] <https://newzoo.com/insights/articles/global-games-market-reaches-99-6-billion-2016-mobile-generating-37/>.
- [42] **Lindsay.** Virtual Reality vs. Augmented Reality. *Augment*. [Online] Augment, 6. 10 2015. [Citace: 8. 10 2016.] <http://www.augment.com/blog/virtual-reality-vs-augmented-reality/>.
- [43] **Ulick, Jaake.** Nintendo Market Value Passes Sony on Pokemon Go Frenzy: Chart. *Bloomberg*. [Online] Bloomberg Technology, 18. 7 2016. [Citace: 8. 10 2016.]

- <https://www.bloomberg.com/news/articles/2016-07-19/nintendo-market-value-passes-sony-on-pokemon-go-frenzy-chart>.
- [44] **Esposito, Nicolass.** *A Short and Simple Definition What a Videogame Is*. University of Technology Compiègne. 2005.
 - [45] **Zimmerman, Eric.** Gaming Literacy Game Design as a Model for Literacy in the Twenty-First Century. 2009, 1, stránky 23-31.
 - [46] **Lowood, Henry E.** Electronic game. *Encyclopaedia Britannica*. [Online] 6. 5 2016. [Citace: 8. 10 2016.] <https://www.britannica.com/topic/electronic-game>.
 - [47] **Kolář, Jaroslav.** *Jak videohry vyprávějí příběhy: Analýza aktuálních klíčových videoher hlavního proudu*. Filozofická fakulta, Masarykova univerzita. Brno : Kolář, Jaroslav, 2013. str. 85, Diplomová práce.
 - [48] **Wikipedia.** Comparison of gaming platforms. *Wikipedia: The Free Encyclopedia*. [Online] 24. 9 2016. [Citace: 14. 10 2016.] https://en.wikipedia.org/wiki/Comparison_of_gaming_platforms.
 - [49] **Maňák, Michal.** Návod, jak začít s Pokémon Go. *DATART*. [Online] 14. 7 2016. [Citace: 14. 10 2016.] https://www.datart.cz/novinky/technologie-pokemon_go.html.
 - [50] *Mobile Market Research, 2014.* **Poynter, Ray.** 6, UK : Market Research Society, 2015, International journal of market research, Sv. 56, str. 705. ISSN 1470-7853.
 - [51] **Wikipedia.** eSports. *Wikipedia*. [Online] 15. 10 2016. [Citace: 16. 10 2016.] https://en.wikipedia.org/wiki/ESports#cite_note-5.
 - [52] **Liquidpedia.** The International. *Liquidpedia*. [Online] 24. 9 2016. [Citace: 16. 10 2016.] http://wiki.teamliquid.net/dota2/The_International#Overview.
 - [53] **Esportsearnings.** E-sports Earnings. *esportsearnings*. [Online] 30. 10 2016. [Citace: 31. 10 2016.] <http://www.esportsearnings.com/>.
 - [54] **Zhou, Ping.** South Korea Computer Gaming Culture. *About Education*. [Online] About Education, 19. 6 2005. [Citace: 16. 10 2016.] <http://geography.about.com/od/culturalgeography/a/South-Korea-Computer-Gaming-Culture.htm>.
 - [55] **GameStart.** Sponsors & Partners. *Game Start*. [Online] Game Start, 24. 2 2012. [Citace: 16. 10 2016.] <http://gamestart.asia/gamestart-2016/sponsors-and-partners/>.

- [56] **GamersApparel.** Partners. *GamersApparel*. [Online] 19. 6 2013. [Citace: 16. 10 2016.] <http://gamersapparel.co.uk/partners>.
- [57] **McKinney, Luke.** 7 Ways Modern Games Have Turned Into Scams. *Cracked*. [Online] Cracked, 22. 3 2015. [Citace: 16. 10 2016.] <http://www.cracked.com/blog/the-6-worst-ways-in-app-purchases-are-ruining-gaming/>.
- [58] **eBay.** Guide to Buying and Selling Online Game Accounts. *eBay*. [Online] eBay, 12. 5 2006. [Citace: 16. 10 2016.] <http://www.ebay.com/gds/Guide-to-Buying-and-Selling-Online-Game-Accounts-/10000000000937297/g.html>.
- [59] **Robin, M.** Been scammed by eBay buyer. *Netmums*. [Online] Netmums, 5. 1 2015. [Citace: 16. 10 2016.] <http://www.netmums.com/coffeehouse/house-garden-194/buying-selling-via-ebay-auction-3rd-party-sites-497/1293247-been-scammed-ebay-buyer-all.html>.
- [60] **elitevppers.** The Black Market. *Elitevppers.de*. [Online] Elitevppers.de, 14. 1 2014. [Citace: 17. 10 2016.] <http://www.elitevppers.com/forum/black-market/>.
- [61] **Dunn, John E.** The top 10 phishing lures of 2015. *Techworld*. [Online] Techworld, 15. 7 2015. [Citace: 8. 10 2016.] <http://www.techworld.com/security/top-10-phishing-lures-of-2015-3620099/>.
- [62] **Federal State Commission.** Consumer Security. *Consumer Information*. [Online] 10. 9 2011. [Citace: 22. 10 2016.] <https://www.consumer.ftc.gov/articles/0009-computer-security>.
- [63] **Hoszowski, Radek.** Bezpečnost, ochrana dat a autorských práv. *sslch.cz*. [Online] 1. 12 2012. [Citace: 26. 10 2016.] <http://www.sslch.cz/files/163/7-bezpecny-pocitac--ochrana-dat-a-autorskych-prav-u.pdf>.
- [64] **AV-Comparative.** Anti-phishing test 2016. *av-comparative.org*. [Online] 22. 6 2016. [Citace: 24. 10 2016.] https://www.av-comparatives.org/wp-content/uploads/2016/07/avc_phi_2016_en.pdf.
- [65] **Steam.** Welcome to Steam. *Steam*. [Online] 12. 9 2003. [Citace: 15. 10 2016.] <http://store.steampowered.com/about/>.
- [66] **Galokin, Sergiy.** Steam Summary for yesterday. *SteamSpy*. [Online] SteamSpy, 24. 3 2015. [Citace: 21. 10 2016.] <https://steamspy.com/>.

- [67] **SteamCharts.** An ongoing analysis of Steam's player numbers. *SteamCharts*. [Online] 12. 4 2012. [Citace: 21. 10 2016.] <http://steamcharts.com/>.
- [68] **Bohemia Interactive.** Bohemia Interactive. *Bohemia Interactive Studio*. [Online] 1999. [Citace: 31. 10 2016.] <https://www.bistudio.com/>.
- [69] **Larabel, Michael.** Steam Crosses 1,500 Games Natively Available For Linux. *Phoronix*. [Online] Phoronix, 19. 9 2015. [Citace: 31. 10 2016.] <https://www.phoronix.com/scan.php?page=article&item=steam-1500-linux&num=1>.
- [70] **Steam.** Steam Support. *Steam*. [Online] 2003. [Citace: 15. 10 2016.] https://support.steampowered.com/kb_cat.php?id=94.
- [71] **Wikipedia.** Smartphone. *Wikipedia*. [Online] 13. 11 2016. [Citace: 15. 11 2016.] <https://cs.wikipedia.org/wiki/Smartphone>.
- [72] **Nowak, Peter.** Video Games turn 50. *CBC News*. [Online] 15. 10 2008. [Citace: 6. 10 2016.] <http://www.cbc.ca/news/technology/video-games-turn-50-1.703624>.
- [73] **Winchester, Henry.** 5 best game download services. *Techradar.pro*. [Online] 24. 1 2012. [Citace: 6. 10 2016.] <http://www.techradar.com/news/computing/pc/5-best-game-download-services-1049981>.
- [74] **Kent, Steven.** *The first quarter: a 25-year history of video games*. 1st, Bothell : BWD Press, 2000. ISBN 9780970475503..
- [75] **Carstensen, Jared.** Cyber Threats & Cybersecurity - Are You Ready? *SlideShare*. [Online] 23. 4 2012. [Citace: 11. 10 2016.] <http://www.slideshare.net/jaredcarst/cyber-threats-cybersecurity-are-you-ready>.
- [76] **NewZoo.** NewZoo. *NewZoo*. [Online] 30. 4 2003. [Citace: 14. 10 2016.] <https://newzoo.com/>.
- [77] **Walrus, Tasty.** Phishing Scams. *Reddit*. [Online] Steam, 17. 5 2016. [Citace: 17. 10 2016.] <https://www.reddit.com/r/Steam/wiki/scamtypes>.
- [78] **Steam.** Account Security Recommendations. *Steam Support*. [Online] 2003. [Citace: 17. 10 2016.] https://support.steampowered.com/kb_article.php?ref=1266-OAFV-8478.
- [79] **malc0de.** BlackLists. *malc0de*. [Online] 24. 10 2016. [Citace: 24. 10 2016.] <http://malc0de.com/database/>.

- [80] **Wikipedia.** Domain Name System. *Wikipedia*. [Online] 13. 11 2016. [Citace: 15. 11 2016.] https://en.wikipedia.org/wiki/Domain_Name_System.

13 SEZNAM OBRÁZKŮ A TABULEK

Obrázek 1 Koloběh spear phishingu [7], přeložil: Autor	5
Obrázek 2 Typ kyberútočníka [75], přeložil: Autor	7
Obrázek 3 Vývojové trendy v zábavním průmyslu [4] [22] [23] [19] [24] [25] [20], zpracoval: Autor	11
Obrázek 4 Vývojový řetězec her, zdroj: Autor	18
Obrázek 5 Vývoj herního trhu [41], přeložil: Autor	19
Obrázek 6 Nejvíce vydělávající hráči, zdroj [53] ,přeložil: Autor	21
Obrázek 7 Metoda MITM, zdroj: Autor.....	26
Obrázek 8 Ukázka blokace jednoho z phishingových webů, zdroj: Autor	30
Obrázek 9 Seznam nebezpečných stránek ze serveru www.malc0de.com [79].....	31
Obrázek 10 Autentizace u KB pomocí SMS, zdroj: Autor	31
Obrázek 11 Ukázka Steam klientu, zdroj: Autor	33
Obrázek 12 Zmenšený Steam klient s přáteli a skupinami online, zdroj: Autor	33
Obrázek 13 Steam trade, zdroj: Autor.....	34
Obrázek 14 Steam uživatelé dle státu ke dni 21. 10. 2016 v procentech, zpracoval: Autor	35
Obrázek 15 Herní rozložení v USA s ČR ke dni 21. 10. 2016 [66], zpracoval Autor	37
Obrázek 16 Původní domény [77]	46
Obrázek 17 Certifikáty v jednotlivých prohlížečích zdroj: Autor.....	46
Obrázek 18 Účet s VAC upozorněním, zdroj: Autor	47
Obrázek 19 Odkaz v e-mailu k verifikaci, zdroj: Autor.....	47
Obrázek 20 Úspěšná validace SteamGuardu, zdroj: Autor	48
Obrázek 21 Vygenerovaný kód na mobilu, zdroj: Autor	48
Obrázek 22 Výzva zadání kódu, zdroj: Autor.....	48
Tabulka 1 Žánry her, zdroj: Autor	17
Tabulka 2 Celosvětová statistika Steam ke dni 21. 10. 2016 v 18h 51min [67], zpracoval Autor ..	36
Tabulka 3 Swot analýza Steamu, zdroj: Autor.....	38
Tabulka 4 Vyhodnocení míry nebezpečnosti útoků, zdroj: Autor	43
Tabulka 5 Bezpečností vyhodnocení útoků, zdroj: Autor	49

14 PŘÍLOHY

14.1 Příloha 1: Phishing odkazy při obchodování

Útok na Steam č. 1 - Phishing odkazy při obchodování					
Položky útoku		Popis			
Cíl		Krádež přihlašovacích údajů na Steamu			
Podmínky		Programování, server hosting, e-mail, Steam účet			
Nástroj rozeslání		Steam chat			
Obsah zprávy		„Ahoj, jmenuji se Petr a viděl jsem tě prodávat věc „X“ za cenu „Y“ ve fóru „V“. Nechtěl bys vyměnit tvoji věc za moji věc „Z“, prosím odešli mi svůj návrh na Steam trade. Díky Můj Steam trade je zde (odkaz na phishingovou stránku)			
Postup		1. Vytvořit stránku na phish Útočník zkopíruje vzhled oficiální logovací stránky Steam (https://steamcommunity.com/login/), poté změní a zprogramuje stránku, tak aby mu poslal přihlašovací údaje oběti. 2. Najít server hosting Útočník si vybere free nebo placenou službu server hostingu. Nejlepší možností pro útočníka je vybrat název, tak aby se, co nejvíce podobal skutečné stránce. 3. Vyhledání oběti Útočník prohledá, dle možnosti, jednotlivé webové stránky s herní tematikou ve formě diskuzí a online fór. 4. Zneužití získaných informací Útočník může využít získané údaje ke krádeži virtuálních věcí na Steam účtu nebo pod tímto účtem, může nalákat přítele oběti, kterého má na Steamu.			
Parametry					
	Váha	Body		Váha	Body
Relevance se Steamem	8 %	2	Rozsah výskytu	10 %	3
Sofistikovanost	5 %	2	Konkrétnost cíle	5 %	2
Délka provedení	10 %	3	Škody	10 %	3
Důvěryhodnost	40 %	3	Opakovatelnost	12 %	2
Vážený průměr parametrů			2.7		
Vybraná bezpečnostní opatření					
Název opatření		Popis		Dostatečné	

Obecné návyky	Rozpoznání phishingové stránky	Ano
E-mailové zabezpečení	Upozornění na návštěvy odkazu	Ano
SteamGuard	Autorizace SteamGuardem	Ano

14.2 Příloha 2: Rychlé prohazování při obchodu

Útok na Steam č. 2 - Rychlé prohazování při obchodu					
Položky útoku		Popis			
Cíl		Krádež virtuálních věcí			
Podmínky		Steam účet			
Nástroj rozeslání		Steam obchod			
Obsah zprávy		Ahoj, vyměním ti věc „X“ za tvoji „Y“. (V tomto případě bývá věc „X“ cennější než věc „Y“, aby oběť souhlasila k obchodu) Díky			
Postup		1. Vyhledat oběť Útočník prohledá uživatele, kteří si chtějí něco vyměnit v online obchodů s virtuálními věcmi na Steamu. Poté si zjistí informací o daném účtu (úroveň účtu, přátelé atd.) a na konec si přidá vyhlédnutou oběť mezi přátele. 2. Zneužití obchodování na Steamu Útočník pošle výhodný obchod oběti, oběť rychle odsouhlasí, ale v tom okamžiku útočník rychle přehodí věc za jinou podobnou. (Útočník může odvést pozornost svými zprávami) 3. Zneužití získaných věcí Ukradené věci si může útočník uchovat pro vlastní potřebu nebo dále prodat.			
Parametry útoku					
	Váha	Body		Váha	Body
Relevance se Steamem	8 %	2	Rozsah výskytu	10 %	3
Sofistikovanost	5 %	1	Konkrétnost cíle	5 %	2
Délka provedení	10 %	3	Škody	10 %	1
Důvěryhodnost	40 %	2	Opakovatelnost	12 %	3
Vážený průměr parametrů			2.17		
Vybraná bezpečnostní opatření					
Název opatření		Popis			Dostatečné
Obecné návyky		Rozpoznání podvodného jednání			Ano
E-mailové zabezpečení		Neupozorní na událost			Ne

SteamGuard	Není využito	Ne
------------	--------------	----

14.3 Příloha 3: Programy ke zlepšení hry

Útok na Steam č. 3 - Programy ke zlepšení hry (Boti)					
Položky útoku		Popis			
Cíl		Krádež herních účtů konkrétní hry			
Podmínky		Herní účet, programovací jazyky k vytvoření aplikace (Bot)			
Nástroj rozeslání		Prostřednictvím hry nebo herních fór			
Obsah zprávy		Ahoj, nebaví tě už dále expit a chceš rychleji získat peníze? Stáhni si bota, který ti pomůže při hraní a ty si můžeš odpočinout. Více informací na této stránce „W“ a hraj zdarma a výhodně.			
Postup		1. Vytvoření herního účtu vybrané hry Je potřeba si zvolit hru, kterou bude útočník využívat. Dále je potřeba herní znalost této hry, aby byl útok relevantní. 2. Vytvoření bota Zde je možnost vytvořit jednoduchou aplikaci, která napodobuje nějakou reálnou aplikaci (naprogramování vzhledu) či vytvořit skutečně fungující aplikaci, ale pak je potřeba vložit více času do naprogramování. 3. Napsat hráčům ve hře Výběr hráče může být náhodný, ale nejlépe se vybírají hráči s nízkou herní úrovní. (Důvod na vylepšení) 4. Stažení bota Oběť po stažení instaluje či spustí program a hraje. Poté, co zadá uživatelské údaje, je možnost pro útočníka počkat na hráče, dokud nebude mít vyšší úroveň a věci, nebo rovnou využije tyto údaje ke svým potřebám. 5. Získané informace Útočník obdrží herní údaje oběti a může ji dále využívat jako vlastní. V nejlepším případě využije účet ke klamavým zprávám přátelům oběti. Díky tomu se program bude šířit dále.			
Parametry					
	Váha	Body		Váha	Body
Relevance se Steamem	8 %	2	Rozsah výskytu	10%	1
Sofistikovanost	5 %	3	Konkrétnost cíle	5 %	2
Délka provedení	10 %	1	Škody	10 %	3
Důvěryhodnost	40 %	2	Opakovatelnost	12 %	3
Vážený průměr parametrů			2.07		

Vybraná bezpečnostní opatření		
Název opatření	Popis	Dostatečné
Obecné návyky	Využití nelegální služby nese rizika	Ne
E-mailové zabezpečení	Upozornění na neautorizované činnosti	Ano
SteamGuard	Autorizace SteamGuardem	Ano

14.4 Příloha 4: Phishingový e-mail od společnosti

Útok na Steam č. 4 - Phishingový e-mail od společnosti					
Položky útoku		Popis			
Cíl		Krádež přihlašovacích údajů na Steamu			
Podmínky		Stejně jako u útoku č. 1 viz Kapitola 14.1			
Nástroj rozeslání		E-mail			
Obsah zprávy		Vážený zákazníku, Zjistili jsme, že se několik cizích počítačů snažilo přihlásit na Váš Steam účet. Potvrďte tyto události nejpozději do 5.11.201x, jinak Vám bude dočasně zablokován účet z bezpečnostních důvodů. Pro potvrzení účtu prosím pokračujte na tento odkaz: (phishingová stránka Steamu) Děkujeme za kontrolu informací a pomoc při udržení bezpečnosti Vašeho účtu. Váš Steam http://www.steampowered.com			
Postup		Postup a obsah je téměř totožný s přílohou 14.1 s jediným rozdílem, kterým je odeslání odkazu přes e-mail. E-mail je zapotřebí získat z herních fór, která umožňují nebo mají možnost nahlédnout na název e-mailu. (Zprávy se odesílají náhodným osobám pod názvem společnosti Steam)			
Parametry					
	Váha	Body		Váha	Body
Relevance se Steamem	8 %	1	Rozsah výskytu	10 %	3
Sofistikovanost	5 %	2	Konkrétnost cíle	5 %	2
Délka provedení	10 %	2	Škody	10 %	3
Důvěryhodnost	40 %	3	Opakovatelnost	12 %	2
Vážený průměr parametrů			2.64		
Vybraná bezpečnostní opatření					
Název opatření		Popis			Dostatečné

Obecné návyky	Rozpoznání phishingové stránky	Ano
E-mailové zabezpečení	Upozornění na návštěvy odkazu	Ano
SteamGuard	Nutná autorizace SteamGuardem	Ano

14.5 Příloha 5: SSFN kód

Útok na Steam č. 5 - SSFN kód					
Položky útoku		Popis			
Cíl		Krádež přihlašovacích údajů Steam			
Podmínky		Steam účet, programovací jazyky k vytvoření webových stránek			
Nástroj rozeslání		Steam Chat			
Obsah zprávy		Viz příloha 14.1			
Postup		1. Vytvoření phishingové stránky Viz příloha 14.1 Oproti prvnímu útoku je zde sofistikovanější programování zapotřebí, Je specifický na zpracování SSFN kódu. Stránka slouží k obcházení Steam Guard autentizace. 2. Vyhledání oběti Výběr oběti na Steamu může být náhodný, hlavním cílem je úspěšné kliknutí na odkaz a doplnění informací. 3. Získání SSFN kódu Stránka bude vyžadovat nahrání SSFN kódu, aby již nadále nemusel být vyplňován kód k autentizaci. 4. Zneužití získaných informací Tento útok obchází veškerá bezpečnostní opatření ze strany Steam, proto jeho následky jsou nejvyšší, neboť útočník má přístup ke všem údajům, a to i platebním, které mohou být na účtu uloženy.			
Parametry					
	Váha	Body		Váha	Body
Relevance se Steamem	8 %	3	Rozsah výskytu	10 %	3
Sofistikovanost	5 %	3	Konkrétnost cíle	5 %	1
Délka provedení	10 %	3	Škody	10 %	3
Důvěryhodnost	40 %	2	Opakovatelnost	12 %	1
Vážený průměr parametrů			2.26		
Vybraná bezpečnostní opatření					
Název opatření		Popis			Dostatečné

Obecné návyky	Rozpoznání nebezpečné stránky	Ano
E-mailové zabezpečení	Útok neupozorní na události	Ne
SteamGuard	Útok obejde SteamGuard	Ne

14.6 Příloha 6: Zneužití jména middlemana

Útok na Steam č. 6 - Zneužití jména middlemana					
Položky útoku		Popis			
Cíl		Krádež virtuálních věcí a herních účtů			
Podmínky		Steam nebo herní účet, pomocník – falešný middleman			
Nástroj rozeslání		Steam obchod, Steam chat			
Obsah zprávy		Dobrý den, jsem oficiální obchodní middleman herních obchodů. Pro recenze navštivte tuto stránku. (oficiální stránka se jménem ověřeného middlemana)			
Postup		1. Vyhledání oběti a poskytnutí služeb middlemana Útočník naláká oběť na obchod a ujistit ho, že z bezpečnostních důvodů je lepší najmout middlemana. Útočník doporučí recenzovaného middlemana a navrhne ho oběti. 2. Vytvoření Steam účtu nebo použití kradených účtů s vyšší úrovní Steam Pomocník útočníka se přejmenuje na middlemana s falešnými recenzemi a napíše oběti, že je připravený k provedení obchodu. 3. Získání virtuálních věcí a účtů Middleman informuje, že již dostal od útočníka věci a čeká se jen na oběť k potvrzení obchodu. Ta odešle věci nebo informace a tímto způsobem je ztratí. Middleman a útočník si mezi sebou prohodí věci a zmizí.			
Parametry					
	Váha	Body		Váha	Body
Relevance se Steamem	8 %	1	Rozsah výskytu	10 %	1
Sofistikovanost	5 %	1	Konkrétnost cíle	5 %	3
Délka provedení	10 %	2	Škody	10 %	2
Důvěryhodnost	40 %	2	Opakovatelnost	12 %	1
Vážený průměr parametrů			1.7		
Vybraná bezpečnostní opatření					
Název opatření		Popis			Dostatečné

Obecné návyky	Rozpoznání podvodného jednání	Ano
E-mailové zabezpečení	Upozornění na nezabezpečené aktivity	Ano
SteamGuard	Není využito	Ne

14.7 Příloha 7: Paypal chargeback

Útok na Steam č. 7 - Paypal chargeback					
Položky útoku		Popis			
Cíl		Krádež virtuálních věcí a herních účtů			
Podmínky		Paypal účet, Steam účet			
Nástroj rozeslání		Jakýkoliv komunikační program			
Obsah zprávy		Ahoj, mám zájem si koupit tvůj účet, který prodáváš přes Paypal.			
Postup		1. Paypal účet Útočník si musí vytvořit účet a mít finanční prostředky na účtu (množství dle potřeby). 2. Potvrzení obchodu Obchod je proveden na koupi herního účtu či virtuální věci na eBay. Útočník pošle peníze na účet, oběť uvidí přijaté peníze a předá svoje zboží přes Steam a veškeré informace k ní potřebné. 3. Zneužití funkce chargeback I když byl obchod úspěšně realizován, útočník může znova vyžádat zpětně svoje peníze kvůli nedoručení sjednané věci, anebo napíše, že byl realizován neautorizovaný obchod. Tímto způsobem jsou obětem odebrány peníze, pokud nemá dostatek důkazů. (Zpravidla velmi těžké, neboť obchod je s virtuálními věcmi a realizován mimo dohlednutí Paypalu)			
Parametry					
	Váha	Body		Váha	Body
Relevance se Steamem	8 %	2	Rozsah výskytu	10 %	1
Sofistikovanost	5 %	2	Konkrétnost cíle	5 %	2
Délka provedení	10 %	2	Škody	10 %	3
Důvěryhodnost	40 %	3	Opakovatelnost	12 %	3
Vážený průměr parametrů			2.52		
Vybraná bezpečnostní opatření					
Název opatření		Popis		Dostatečné	
Obecné návyky		Riziko ztráty je součástí obchodu		Ne	

E-mailové zabezpečení	Neupozorní na situaci	Ne
SteamGuard	Není využito	Ne

14.8 Příloha 8: In-game scam

Útok na Steam č. 8 - In-game scam					
Položky útoku		Popis			
Cíl		Krádež virtuálních věcí a peněz			
Podmínky		Herní účet			
Nástroj rozeslání		Zpráva prostřednictvím hry			
Obsah zprávy		Ahoj, nabízím ti tyto služby (pomoc splnění herního úkolu, mise nebo dobytí) nebo powerlevel stačí, když mi zaplatíš „X“ cenu za hodiny. Služba je non-stop!			
Postup		1. Herní účet Nejprve musí mít útočník několik herních účtů za účelem recenzovat služby z hlediska důvěryhodnosti jiného účtu útočníka, který bývá zpravidla na vysoké herní úrovni. 2. Nalákat oběť Oběť uvidí účet, který tyto služby poskytuje, zeptá se ostatních účastníků (zpravidla útočníkovi pomocníci nebo o sám). Oběť odsouhlasí a předá peníze. 3. Zneužití Peníze jsou většinou pro oběť ztraceny, i kdyby se dožadovala vrácení peněz přes administrátory her, bude oběť, u většiny případů, obeznámena o své nedbalosti aniž by byla nějak uhrazena. Jediná záchrana je v podobě důkazů detailního popisu doplněné o screenshoty.			
Parametry					
	Váha	Body		Váha	Body
Relevance se Steamem	8%	1	Rozsah výskytu	10 %	3
Sofistikovanost	5 %	2	Konkrétnost cíle	5 %	2
Délka provedení	10 %	2	Škody	10 %	1
Důvěryhodnost	40 %	1	Opakovatelnost	12 %	2
Vážený průměr parametrů			1.52		
Vybraná bezpečnostní opatření					
Název opatření		Popis			Dostatečné

Obecné návyky	Rozpoznání herního scamu	Ano
E-mailové zabezpečení	Neupozorní na událost	Ne
SteamGuard	Není využito	Ne