Bezpečnost v kyberprostoru

Moravcová, Záveská

Studijní materiál vznikl za podpory projektu
Vzájemným učením - cool pedagog 21. století (CZ.1.07/1.3.00/51.0007), který je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Význam ikon v textu

Cíle
Na začátku každé kapitoly je uveden seznam cílů

Pojmy k zapamatování
Seznam důležitých pojmů a hlavních bodů, které by student při studiu tématu neměl opomenout.

Poznámka
V poznámce jsou různé méně důležité nebo upřesňující informace.

Kontrolní otázky
Prověřují, do jaké míry student text a problematiku pochopil, zapamatoval si podstatné a důležité informace.

Souhrn
Shrnutí tématu.

Literatura, zajímavé odkazy
Použitá ve studijním materiálu, pro doplnění a rozšíření poznatků.

Obsah

1 Úvod

Internet představuje relativně nové dynamické prostředí se specifickými normami, které se často velmi liší od norem offline světa. Je multifunkčním prostředím, které svým uživatelům poskytuje nástroje ke vzdělávání, komunikaci či rozvoji pracovních a obchodních aktivit. Mimo to nabízí rovněž prostor k relaxaci a kulturnímu vyžití.

Kromě nesporných výhod však s sebou toto rychle reagující a vyvíjející se prostředí nese řadu rizik a skrytých hrozeb často podceňovaných uživateli. Jako skutečný problém se jeví právě jejich netečnost. Proto je třeba porozumět nejen těmto rizikům, ale také chování uživatelů v online prostředí.

Rizika můžeme vnímat ve dvou rovinách – v rovině technologické a lidské. K technologickým rizikům řadíme činnost, která prostřednictvím tvorby software útočí na zranitelná místa počítačů s cílem získat a zneužít data, citlivé údaje, popřípadě se obohatit na úkor napadeného uživatele.

V rovině lidské se nejedná o útok na technické vybavení, ale na konkrétního jedince rozvíjejícího svou identitu v kyberprostoru v rámci sociálních sítí, chatů, her a jiných platforem. Při střetu s tímto nebezpečím může jedinec utrpět újmu ve sféře psychické i fyzické.

1.1 Tvorba hesel

Základním bodem prevence před zneužitím internetové identity a ztráty dat je výběr a užití vhodného přístupového hesla. Takové heslo by mělo obsahovat kombinace čtyř skupin znaků: malých a velkých písmen obou velikostí, číslic a ostatních symbolů. Zdroj uvádí nutnou délku bezpečného hesla alespoň osm číslic, jako optimální se jeví délka čtrnáct a více znaků. Jak bylo uvedeno, heslo by mělo obsahovat čtyři skupiny znaků. Absence některé skupiny zvyšuje nároky na počet znaků (Bezpečný internet [b. r.].

Je sice dobré používat speciální znaky, ale je třeba zvážit, kde všude bude uživatel zadávat heslo, a promyslet možnosti tamní klávesnice. Je totiž možné, že se bude uživatel chtít přihlásit na některý ze svých účtů, ale nebude mu to dopřáno kvůli absenci některých kláves. Uživatel by měl vzít v potaz také to, že používání běžných slov a různých důležitých údajů z osobního života může být velmi rizikové. Běžně používaná slova jsou prolomitelná takzvanou slovníkovou metodou, kdy je specializovaný software schopen odhalit toto heslo. Souznění hesla a uživatelského jména se rovněž jeví jako poměrně krátkozraké (Kozák 2008).

K vytvoření neprolomitelného hesla lze využít různé programy, které heslo vygenerují. Tento software má v sobě implementovaný například operační systém Linux. Existují i generátory hesel na webu. Jejich použití je ale poměrně sporné. Uživatel nemá nikdy záruku toho, že si administrátor takového webu nevytváří databáze hesel. Zdroj hovoří o tom, že ve spojení s IP adresou může docházet k získání přihlašovacích údajů (Kozák 2008).

Po vytvoření bezpečného hesla je nutné toto heslo co nejlépe chránit. Pokud si není člověk schopen heslo pamatovat, doporučuje se hlavně ho nikam nezapisovat. K tomuto účelu lze využít speciální software. Dalším pochybením je zaslat v případě potřeby heslo další osobě, navíc ještě po emailu, nebo SMS. Je také třeba používat pro přihlašování zabezpečené protokoly, zdroj zmiňuje protokol SSL, který se na počátku webové adresy projevuje jako "https://". Heslo je také třeba často měnit, někteří správci firemních systémů toto vyžadují například po třech měsících. Samozřejmostí je tvořit pokaždé nové heslo, je to sice náročné, ale i tak si lze najít systém. Pokud je třeba, aby se nějaká jiná osoba připojila k vašemu uživatelskému účtu, je dobré využívat takzvaných OTP (=One-time Password). Jak napovídá název, jde o heslo na jedno přihlášení (Kozák 2008).

2 Viry a škodlivý software

Cíle

Po prostudování této kapitoly:

- Získáte přehled o druzích virů, červech a trojských koních.
- Naučíte se rozpoznat, co který druh škodlivého software způsobuje.

Pojmy k zapamatování

- Vir
- Stealth vir
- Botnet
- Replikace virů
- Polymorfní vir
- Červ
- DDoS útok

2.1 Viry

Viry jsou druhem software, kterým se infikuje počítač uživatele. Většinou se tak děje následkem neopatrného nebo ne zcela bezpečného chování. Mezi takové druhy chování patří například absence zabezpečení počítače nebo počítačové sítě, ignorace upozornění antiviru, návštěvy vybraných webových stránek, popřípadě otevírání a manipulace s přílohami emailů od neznámých odesilatelů.

Počítačový virus je program, který je připojen k některému ze spustitelných souborů, popřípadě k některému z dokumentů. Program je při spuštění, nebo otevření takového souboru spuštěn a začne konat svou činnost. Virus má také mimo jiné schopnost se množit a nakazit další soubory, se kterými se také šíří při jejich sdílení. Tato schopnost se nazývá **replikace** a probíhá tak, že virus je schopen se namnožit při spuštění souboru, který infikoval.

Způsobů, kterým jsou viry děleny, je vícero. Pro účely tohoto textu byl vybrán způsob, jímž viry dělí Požár. Dle něj jsou děleny do několika kategorií, jejichž přehled přináší tabulka, každá z kategorií bude dále vysvětlena.

Kategorie	Skupiny
Dle umístění v paměti	· Rezidentní; · Nerezidentní
Dle zacílení infekce	· Souborový; · Bootový; · Clusterový; · Multiparitní
Dle chování v systému	· Worm; · Stealth vir; · Polymorfní vir; · Trojský kůň

Tabulka 1 – Dělení počítačových virů dle kategorií

Zdroj: (Požár 2007, 46), upraveno

Prvním hlediskem dělení počítačových virů je tedy to, jak se staví k operační paměti. **Rezidentní viry** jsou spuštěny a zůstávají v paměti a mohou tedy infikovat jakýkoliv soubor. Dle zdroje spočívá princip rezidentního viru v tom, že je jeho replikační modul nahrán do paměti a činnost viru je spuštěna při provedení určité akce operačního systému, například načtení. Tento typ je horší v tom, že nakazí, jak již bylo uvedeno, v podstatě jakýkoliv soubor. Rezidentní viry lze dále dělit na rychle a pomalu infikující. Antivirový program je schopen zachytit první typ rychleji, protože ten se snaží za menší čas nadělat více škody, oproti tomu druhý typ je zachycen za delší dobu, protože jeho působení v systému není tak nápadné, jak opět uvádí zdroj. Oproti tomu **nerezidentní viry** jsou spouštěny vždy s určitým souborem. To znamená, že nejdřív je spuštěn soubor, a poté může teprve virus infikovat soubory. (Techopedia ©2010-2015)

Další náhled poskytuje rozdělení virů podle cíle infekce. Jde tedy opět o cílové umístění viru, tentokráte ale z jiného pohledu. Prvním typem jsou **souborové viry**, které napadají spustitelné soubory. To znamená, že napadnou soubor, ve kterém je nějaký kód. Podle toho také bývají děleny na nepřepisující a přepisující viry. V obou případech virus doplní svůj kód do kódu souboru, liší se pouze přístup k němu. U nepřepisující varianty nenahrazuje kód viru kód původního souboru, pouze v hlavičce původního souboru je umístěn odkaz na nový škodlivý kód. Program tedy započne svou činnost a vykoná tělo viru. Uživatel nemá moc tolik šancí poznat, že je něco v nepořádku. Kdežto u přepisující varianty je odhalení o poznání snazší, neboť virus přepíše rovnou kód původního programu, který potom nemůže být vykonán. Uživatel tedy spustí program, je proveden kód viru a původní program nevykoná svou činnost, protože jeho kód byl nahrazen. Uživatel tedy může rozeznat, že je něco v nepořádku. (TrustPort 2010)

"Boot sektorové viry infikují proveditelný kód nacházející se v určitých systémových oblastech na disku. Těmito oblastmi mohou být boot sektory disket, tabulka rozdělení pevného disku nebo boot sektor pevného disku. Boot sektor existuje na každé disketě, která byla naformátována pomocí MS-DOS, a to bez ohledu na to, zda touto disketou je systémový nebo datový disk. Boot sektor obsahuje krátký program, který používá DOS ke spuštění systému, a to dříve než je kontrola předána jiným systémovým programům a překladači povelů." (TrustPort 2010)

Z uvedeného textu vyplývá, že **bootový virus** je výrazem spíše minulosti, pro úplnost byl ale v tomto textu uveden, stejně tak jako jeho princip. Ten spočívá v tom, že při startu počítače je uveden do provozu nejdříve bootovací mechanismus, jež načte do paměti instrukce nutné ke startu počítače a operačního systému, který pak přebere svou funkci prostředníka mezi programy a hardwarem. Tady nastává prostor pro virus, který je při nabootování z diskety naveden do paměti, respektive je naveden hlavně odkaz na jeho umístění, což znamená, že při nabootování počítače je virus stále zaváděn do paměti a mohl tak nakazit další a další diskety a jejich prostřednictvím i další počítače. Zdroj dále uvádí, že se tento vir uplatňoval zejména v operačním systému MS-DOS, ve 32 a 64bitových systémech bývá tento vir snadněji odhalitelný. Znalost bootovacích virů spíše slouží jako podklad pro znalost multiparitních virů. (TrustPort 2010)

Pevný disk v počítači je v logické rovině dělen na části, takzvané clustery. Na tyto části se orientují **clusterové viry**. *"Clusterové viry neprovádějí změny v souborech, ale mění informace v adresářové položce daného programu. Modifikují odkazy adresářové struktury, aby ukazovaly na kopii infikovaného kódu."* (Koláček 2009)

Princip nákazy počítače clusterovým virem je takový, že virus na nějakém místě na disku uloží svůj kód. Pro tento účel si vybírá místo nenápadné, aby nemohl být tak dobře odhalen, a poté změní odkaz na soubor v adresářové struktuře. Uživatel spustí daný soubor, nejdříve jsou provedeny instrukce v kódu viru a pak je spuštěn samotný soubor. (Koláček 2009)

Poslední ze skupiny virů dělených dle cíle infekce jsou takzvané **multiparitní viry**. Multiparitní v tomto případě znamená, že vir je schopen infikovat portfolio souborů zahrnující soubory spustitelné i bootovací sektory disku. Princip jeho fungování je opět jednoduchý. Uživatel spustí program s virem, který okamžitě zařídí zápis do bootovacího sektoru, což znamená, že virus při opětovném nabootování, nelimitovaném počtem provedení, může nakazit každou libovolnou aplikaci. (TrustPort 2010)

Poslední z kategorií je rozdělení dle toho, jak se virus v systému chová. Jedná se o kategorii na popis nejbohatší. Jak bylo uvedeno v tabulce, tak do této kategorie patří worm programy, neboli červi; stealth viry; polymorfní viry a trojské koně. O každé skupině virů bude dále v textu řeč.

2.2 Worm

Červ, jak zní překlad slova worm, se v některých ohledech podobá a v některých liší od viru. Tyto charakteristiky budou dále rozebrány. Červ umí sám sebe kopírovat a také umí vyvinout záškodnickou činnost jako samotný virus. V případě „benigního“ červa se jen volně množí a cestuje po síti, neškodí ale nikomu svou činností. Hlavní rozdíly spočívají ve schopnosti cestování a ve vztahu s hostitelem. Červ je totiž sám o sobě spustitelným souborem, nemusí tedy šířit nákazu na jiné soubory po okolí. Má také schopnost zmapovat počítačovou síť a dle aktivity vyhodnocuje, kam sám sebe zkopíruje a rozšíří tím nákazu. (Peterka 1994)

Při svém cestování po síti červ zneužívá nezabezpečené systémy, do kterých může proniknout. Jako další výhoda se jeví schopnost přesvědčit uživatele o tom, že červa spustí. K tomu může docházet například při stažení různých utilit a programků, které chce uživatel vyzkoušet, neboť o nich na internetu našel kladné recenze. Ty pak mohou být červem, kterým si nakazí počítač. Zmíněná schopnost manipulace s uživateli staví na takzvaném sociálním inženýrství. To staví na tom, že buď uživatel provádí chtěnou interakci, nebo alespoň vyzradí některé z citlivých údajů. Takto získaná data a citlivé údaje potom tvůrci červů využívají k nekalé činnosti. (Cisco [b.r.])

Červy můžeme dle zdroje dělit na emailové, internetové, IM a IRC a červy využívající sdíleného prostoru. Každý z těchto druhů má svá specifika, o kterých bude dále řeč.

Emailového červa, jak již napovídá název, lze získat při otevření nakažené přílohy emailu, takže nákaza se může s dnešní dostupností internetového připojení a elektronické pošty velice rychle. Pokud dojde k nákaze, červ projde celý adresář uživatele a odešle se každému kontaktu. (Firetrust 2015)

Internetový, neboli **síťový červ** se šíří po místních sítích (LAN) a nebo po intranetu. Je tedy zaměřen na korporátní sféru. Pokud se nějaký počítač připojí k jinému nakaženému počítači, nebo serveru, okamžitě je také nakažen. Poté se obvykle zkopíruje ke každému uživateli zvlášť (okupuje spouštěcí složky) a může být tedy spuštěn při každém přihlášení. Tito červi navíc umí najít hůře zabezpečený přístupný bod, popřípadě úložiště dat, přes který vniknou do firemní počítačové sítě, nebo zvládají získat hesla k zabezpečeným úložištím. Navíc jako bonus k nim mohou být připojeni keyloggery, nebo další software, který umí komunikovat se vzdálenějšími servery. (F-secure [b.r.])

Síťového červa spolu s například keyloggery mohou hackeři využívat například k průmyslové špionáži, o čemž bude ještě řeč.

Další skupinou jsou **IM a IRC červi**, kteří se zaměřují na rychlé zprávy (takzvaný Instant Messaging), nebo chat (Internet Relay Chat). Princip činnosti IM červa je podobný jako v případě emailového červa. Opět tedy po propuknutí infekce červ projde kontakty a rozesílá na ně své kopie. Cílový uživatel si mylně může vyložit, že mu píše někdo z jeho přátel a nakaženou zprávu otevře. Ve zprávě není zpravidla text, ale odkazy na různé webové stránky. Důvodem vzniku tohoto typu červa je zejména finanční výdělek. Příkladem může být takzvaný TheChoke, který v komunikaci přes MSN Messenger nabízel odkazy na stažení různých utilit. Tento odkaz byl ovšem podvrh a jednalo se o odkaz na stažení samotného červa. Daleko nebezpečnější ovšem je takzvaný SoFunny, který se objevil v AOL Messengeru. Ten umí vylákat přihlašovací údaje a potřebná hesla a odeslat je poté na daný podvržený email. Na rozdíl od ostatních červů ale není tak snadno odhalitelný, protože ho nelze identifikovat systémem a nezobrazí se jako aktivní ve správci úloh. (Techopedia ©2010-2015)

IRC červi neprojevují takovou účinnost jako IM červi. Šíří se zejména přes různá diskuzní fóra a chaty a na nich rozesílá buď infikované soubory, nebo odkazy na pochybné webové stránky. Jeho malá účinnost spočívá zejména v tom, že příjemce nejdřív akceptuje dodaný soubor, uloží ho a otevře a až poté může dojít k rozšíření nákazy. Zpomalení také vznikne jeho další funkcí. Připojí se pomocí klienta nakaženého uživatele k IRC serveru, poté vybere vlákno, které infikuje a nakonec rozesílá sám sebe všem, kdo se zrovna účastní dané diskuze. Hodí se tedy spíš jako jakási brána pro vstup dalšího nežádoucího, škodlivého a zákeřného software. Tento druh červa je zacílen spíše na chatovací klienty, kteří umožňují nastavení přijímání souborů, jež není nutné předem potvrdit. (Techopedia ©2010-2015)

Poslední skupinou jsou **červi**, kteří se množí **ve sdíleném prostoru.** Jednou z cest je zkopírování souboru s červem do sdílené složky, ze které ho mohou libovolní uživatelé stáhnout a opět spustit, aby mohlo dojít k nakažení. Další cestou jsou P2P, neboli Peer-to-Peer sítě. Ty fungují tak, že v libovolném okamžiku je vždy některý sdílející počítač pro ostatní serverem, ke kterému přistupují, zpravidla přes nějakého klienta. Červí soubor bývá navíc zpravidla pojmenován pro uživatele atraktivním názvem, buď jako doplněk nějaké hry, popřípadě některá ze sledovaných relací. Uživatel s nadšením soubor stáhne a místo obsahu slíbeného v názvu se dočká jen nakaženého počítače. Červ navíc vyhledává další a další oběti. (F-secure [b.r.])

2.3 Stealth vir

Jak již bylo uvedeno, viry se musí infiltrovat na některý ze souborů v počítači, aby mohli existovat. Jedním z druhů virů je takzvaný stealth virus, který si klade za cíl co nejdéle se skrývat před objevením a odstraněním. Provádí to velice důmyslnou cestou a to tak, že v sobě uchovává obsah původního nenapadeného souboru. Pokud zjistí, že je počítač prohledáván antivirem, tak se pro tento jeví jako původní soubor, tedy mu ukáže obsah souboru takový, jaký byl původně. Díky této maskovací taktice trvá antivirovému programu podstatně déle, než ho objeví, popřípadě odstraní. Antivirový program sice umí rozpoznat, že se v počítači děje něco nekalého, ale stealth vir nakazí jiný soubor a místo původního vytvoří prázdný soubor. Navíc umí naoko zaměnit i velikost souboru, který nakazil. Díky tomu antivir nemůže poznat změny. Touto svou aktivitou samozřejmě nepřímo úměrně klesá výkon počítače, jak uvádí zdroj. (Kaspersky Lab ©1997-2015a)

Dále také uvádí, že stealth vir se do počítače obvykle dostane z nakaženého emailu, nebo spuštěním zavirovaného software. Postup k odstranění je následující: nabootování napadeného počítače z jiného disku a následná důkladná kontrola diskové jednotky antivirovým programem. Na něj je kladen požadavek, aby byl schopen nalézt kompletně všechny části viry, které vznikly při kopírování a maskování. (Kaspersky Lab ©1997-2015a)

Další neviditelné techniky, které stealth viry ovládají, jsou řízení služeb operačního systému, což také zatěžuje výpočetní kapacity počítače a ovlivňuje jeho výkon. Antiviry se proti tomuto počínání snaží bojovat naopak anti-stealth technikami, kdy potřebné vybrané soubory kontrolují podle toho, jak jsou uloženy v ROM paměti, kde nedochází k modifikacím. (Matějka [b.r.])

2.4 Polymorfní vir

Tyto typy virové nákazy se také snaží svými taktikami skrývat před objevením, což mají stejné se skupinou stealth virů. Mechanismus mají ovšem docela jiný. Umí totiž své kopie modifikovat tak, aby byly navzájem na první pohled neporovnatelné. Další a další kopie jsou vždy jen variantou svých předchůdců. Aby nemohlo docházet k odhalení, tak nemají shodné části kódu. Navíc i kódování je pro každého potomka jiné. Celým tímto mechanismem dochází k tomu, že je také horší jej odhalit, jak uvádí zdroj. (Computer hope ©2015)

Další ze zdrojů uvádí, že i přes množství variant, které vznikají kopírovacím mechanismem, je původní smysl, který je vyjádřený v tomto případě nějakým algoritmem, stejný jako na počátku. Funkcionalita je tedy zachována, jen je vyjádřena v kódu jinou posloupností příkazů, protože u programování platí zvláště, že nemusí existovat jen jedna jediná správná cesta k cíli. (Cknow 2013)

2.5 Trojský kůň

Trojský kůň představuje takový obtěžující software, který se lstí dostane do operačního systému uživatele (podobným algoritmem jako v případě obléhání Tróje z řeckých bájí). Jak uvádí zdroj, trojský kůň patří mezi takzvané červy. Dále říká, že se navenek trojský kůň tváří jako nějaká aplikace, která má uživateli pomoct, v nitru ale obsahuje kód s úplně jinou funkčností, než sliboval. V systému pak provádí záškodnickou činnost podle toho, o který druh se jedná. (Lupa ©1998-2015)

Pro účely tohoto textu jsem trojské koně rozdělila do sedmi skupin podle toho, který druh záškodnické činnosti na nakaženém počítači provádí. Každá skupina bude probrána zvlášť. Vycházím ze seznamu a definic na stránkách společnosti **Kaspersky** (Kaspersky Lab ©1997-2015b), pokud neuvádím jiný zdroj, který jsem doplnila o informace o některých virech. Tato společnost se zabývá vývojem a prodejem software pro ochranu počítačů a sítí.

Prvním typem je *"trojský kůň pro síťové **ovládání vzdáleného systému**"*. (Bitto 2005) Jak napovídá název, jedná se o program, s jehož pomocí lze získat moc nad nakaženým počítačem. Dle serveru lupa.cz komunikuje přes porty neblokované firewallem, o němž bude některá z dalších kapitol tohoto textu. Zdroj dále uvádí třístupňovou ochranu proti trojskému koni. (Lupa ©1998-2015)

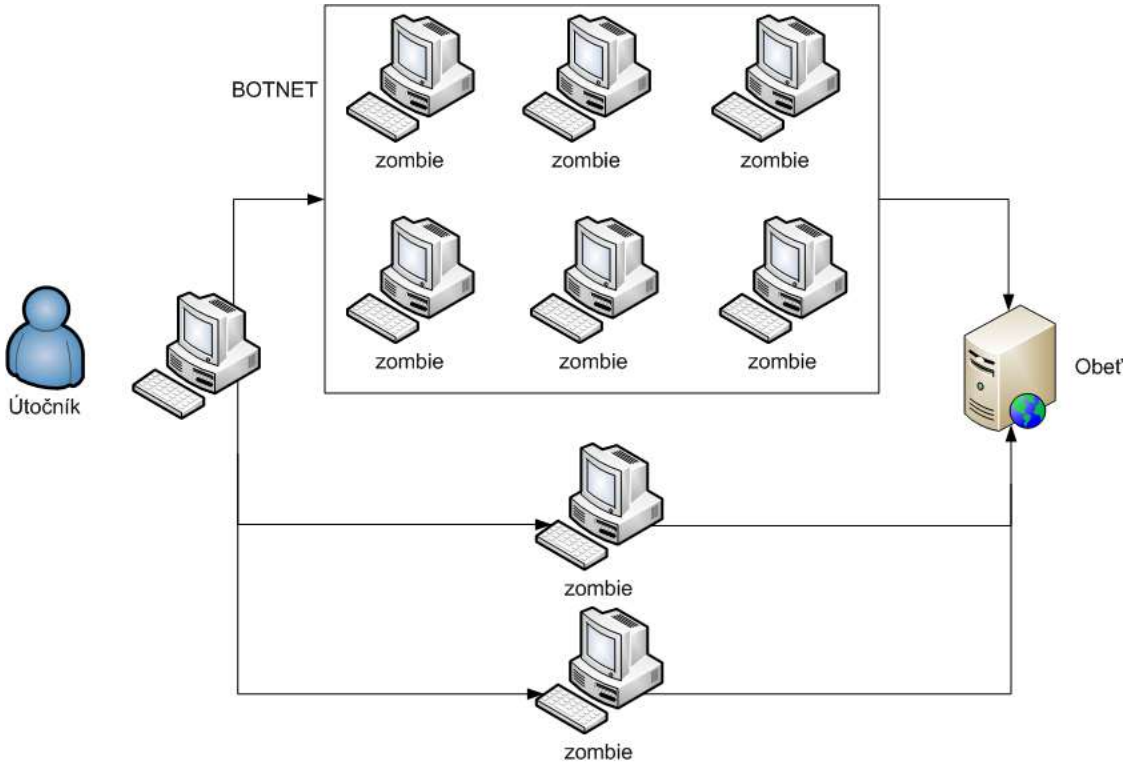
Prvním krokem je využití selského rozumu uživatele. Je nutné přemýšlet o tom, které servery navštěvujeme, popřípadě jaké soubory a programy stahujeme a spouštíme v počítači. Dalším krokem je využívání antiviru, o němž bude také pojednávat jedna z dalších kapitol. Antiviry mají některé trojské koně ve svých virových databázích, proto je umí rozpoznat. Posledním, neméně důležitým, krokem je využívání a správné nastavení firewall. Jak již bylo uvedeno, trojský kůň využívá některé z neblokovaných portů, proto je nutné tyto porty znát a správně je nakonfigurovat. Trojský kůň tohoto typu je spouštěn po startu systému, znamená to tedy, že se bez výjimky spouští pokaždé. Do této skupiny patří například: **Zadní vrátka, ArcBomb,** nebo **Proxy.** Zadní vrátka jsou, dle serveru Kaspersky, využívána pro řízení vzdáleného počítače: "*trojské koně s funkcí zadních vrátek často slouží ke sjednocení skupiny nakažených počítačů, které vytvoří botnet, neboli zombie síť, kterou lze využívat k nezákonným účelům."* (F-secure [b.r.]) Podobně se chová trojský kůň nesoucí název Proxy, který dle zdroje slouží k vytvoření proxy spojení, čímž se stává vystopovatelným nakažený počítač, nikoliv počítač skutečného záškodníka. Třetí ve skupině je ArcBomb, který sem byl zařazen, protože snižuje výkon počítače archivy bez hodnoty pro uživatele. Dle zdroje je typicky využíván k zahlcení emailového serveru, ale může zahltit i samotný počítač. (Kaspersky Lab ZAO ©1997-2015a)

Druhou skupinou je vyhledávání zranitelných míst a jejich další manipulace, patří sem kupříkladu: **Exploit**, **Rootkit** a **Dropper**. Tyto trojské koněkryjí záškodnické chování ostatního software, zametají stopy a prodlužují dobu nutnou pro nalezení tohoto software. Slouží hlavně jako jakási "zástěrka", nebo klam, k další činnosti a instalaci dalších škodlivých programů.

Třetí skupinu tvoří trojské koně, které jsou spouštěny zpravidla jen jednou, jak uvádí jeden ze zdrojů. (Bitto 2005) Neznamená to ale, že je o něco méně škodlivý. Jde o tyto typy: **Banker**, **Game Thief**, **IM**, **Spy**, **Mailfinder** a **Notifier**. Všechny mají společné to, že se snaží odcizit přihlašovací údaje a hesla, liší se pouze tím, k jakému účtu. Jak napovídá název, u typu Banker jde o odcizení přihlašovacích údajů k internetovému bankovnictví. Game Thief, který pochází z rodiny trojských koňů s názvem PSW, slouží k ukradení identity ve světě online her. (F-secure [b.r.]) U IM jde o údaje k účtům v programech k zasílání zpráv (= Instant Messaging). Spy, jak opět napovídá název, sleduje buď uživatele samotného, nebo jeho práci a pohyb pomocí periferních zařízení (typicky web kamera nebo klávesnice). Pomocí Mailfinderu mohou zase hackeři získat spousty emailových adres, které potom mohou využít typicky k rozesílání SPAMu, o němž bude dále řeč. Posledním ze skupiny je Notifier, který funguje trochu jinak. Dle zdroje (Kaspersky Lab ZAO ©1997-2015b) totiž shromažďuje informace o počítači a jeho připojení k síti, což znamená IP adresu, potom volné porty a jiné další informace o komunikaci. Koně z této skupiny typicky informují hackera emailem, popřípadě nějakým jiným komunikačním kanálem.

Samostatnou skupinu tvoří trojské koně k vyvolání **DDoS** útoků. Ty se zpravidla cílí na některý web za účelem ho zahltit z různých počítačů tolika žádostmi o připojení, až dojde k tzv. odmítnutí služby. Pod označením DDoS (=DistributedDenialafService) si lze představit takové počínání, které vede k zahlcování provozu na serveru, čímž dochází v daný okamžik k vyčerpání jeho kapacity a neschopnosti obsloužit požadavky ostatních uživatelů. Útočník tedy dosahuje svého tím, že dojde ke kolapsu služby. DDoS útoky lze také popsat pomocí zahlcování emailové schránky zasláním velkého množství emailů, jak uvádí zdroj[24]. Zvláště v dřívějších dobách, kdy měly emailové schránky velmi omezenou kapacitu, mohl tento trojský kůň být velice účinným nástrojem. (ITbiz [b.r.])

Vedle DDoS útoků ještě existují takzvané DoS útoky. Jejich princip fungování je stejný, liší se pouze počtem počítačů zapojených do takzvané "zombie" sítě. Při DoS útoku je využit pouze jeden stroj, ve druhém případě jich je využito více (odtud distribuovaný ve smyslu rozdělený mezi více strojů). DoS (= DenialofService) lze tedy plně definovat jako: *"znepřístupnění služeb a to jakýmkoliv způsobem. Od vytržení kabelu ze serveru po využití slabiny v aplikaci, kdy po odeslání specifického řetězce server vytuhne a přestane komunikovat. Může se jednat o využití chyby, dosažení limitu systému, síťové karty, aplikace, nebo systémových prostředků jako je CPU, paměť, místo na disku, či IO operace. Pokaždé, když je výsledkem útoku nedostupnost služby daného serveru, tak se jedná o DoS."* (Čmelík 2013) Z uvedeného tedy vyplývá, že DoS útok je ve své podstatě útok na kteroukoliv součást systému, jak hardwarovou, tak i softwarovou. Jak již bylo uvedeno, jsou při těchto útocích využívány "zombie" sítě, které jsou vidět na Obrázku 1.



Obrázek 1 – Schéma DDoS útoku

Zdroj: <http://www.shiba-inu.sk/matej/index.php?kap=protect>.

Na obrázku je viditelné schéma DDoS útoku, v jehož čele stojí Útočník, který ovládá zombie počítače buď napřímo, nebo přes takzvané handlery, jež ještě více znemožňují odkrytí útočníka. Handlery jsou vlastně takovým prostředníkem, neboli bránou, která spojuje zombie síť a útočníka, která navíc podle pokynů útočníka řídí zombie síť. (Mihalech ©2015) Na druhém okraji stojí server Oběti, který, pokud není dobře chráněn, je vyřazen z provozu buď celý, nebo některá z poskytovaných služeb. Vedle samotných zombie počítačů je na schématu zobrazen ještě botnet, tedy síť, o níž bude ještě řeč. Problematika DDoS útoků je poměrně rozsáhlá, proto pro úplné pochopení doporučuji nastudovat některé ze zdrojů.

Pátou skupinou jsou trojské koně zaměřené na připojování se na určité weby, popřípadě stahování nevyžádaných dat. Představiteli této skupiny jsou: **Downloader** a **Clicker.** Downloadery stahují další a další nevyžádané a škodlivé programy a starají se o jejich úspěšnou instalaci. Clickery se dle zdroje snaží o zpeněžené připojování k určitým stránkám. (F-secure [b.r.])

Představiteli předposlední skupiny jsou: **FakeAV** a **Ransom**. Jde o trojské koně sloužící k vymáhání peněz pod určitou smyšlenou hrozbou. FakeAV, jak napovídá název, slouží hlavně k podnícení jakési smyšlené detekce různých virů antivirovým systémem nainstalovaným v počítači. Samozřejmě nabízí za úplatu odstranění těchto různých virů a dalších ohrožení. Oproti tomu Ransom slouží k modifikaci jakýchkoliv dat na počítači, jejímž následkem jsou nepřístupná, nebo se programy a operační systém jako takový mohou chovat nestandardním způsobem. Problémy s daty je možné odstranit opět za úplatu.

Trojské koně neohrožují jenom počítače, ale i další mobilní zařízení. Představitel poslední skupiny nese název **SMS**. Jak napovídá název, jedná se o trojského koně, který zasílá krátké textové zprávy na různá prémiová čísla, nebo čísla uložená v mobilním telefonu.

Kapitola o trojských koních nenese za hlavní cíl dopodrobna rozebrat každého trojského koně, který vznikl. Cílem bylo, aby čtenáři získali povědomí o tomto druhu škodlivého software a získali představu o skutečně rozmanité činnosti. Jak již bylo uvedeno, je nutné k obsahu putujícímu po webu i samotným webovým stránkám přistupovat s rozmyslem a zběsile nenavštěvovat každý web, který slibuje nevšední zážitky. I když i odstraňování nežádoucího software a získávání ztracených dat a identity může být také nevšedním zážitkem.

2.6 Botnet

Jak již bylo uvedeno, botnet je využíván například ve spojitosti s DDoS útoky. Hlavním motivem pro vytvoření botnetu není ale útočit na servery, nýbrž pronajmout různě velkou infrastrukturu k některým činnostem. Pokud se teď odpoutáme od myšlenky, že botnety využívají pronajímatelé zejména k zasílání SPAMu, o němž bude ještě řeč, DDoS útokům, jak ukazuje obrázek 1, popřípadě jiným nekalým činnostem, můžeme najít i jeho kladné stránky. Botnet lze ve správných rukách využít kupříkladu k činnostem náročným na výpočetní kapacity, jako jsou třeba složité výpočty používané pro počítačovou grafiku.

Botnety jsou ale ze své podstaty využívány spíše k nekalým činnostem, jak napovídá i jejich tajné vytvoření, k němuž jsou využívány zejména trojské koně, jak uvádí zdroj. (Wikipedie [b.r.]) Botnet vznikne tak, že jeho správce, vytipuje nechráněné počítače, jež nakazí, jak již bylo uvedeno, trojským koněm. Způsoby nákazy trojským koněm, nebo kombinacemi několika z nich jsou různé, například po síti, nebo přes USB disky. Když je tato síť funkční a zavedená, může její správce část pronajmout, například k DDoS útoku, nebo posílání SPAMu, popřípadě hrozeb na vymáhání peněz. Důvody k vytvoření botnetumohou být různé, společné mají ovšem to, že pronajimatel šetří náklady za vytvoření a zprovoznění složité počítačové infrastruktury s odpovídajícím výkonem a zároveň je chráněn, pokud by měl být z nějakého důvodu vystopován.

Pod slovem bot se skrývá zkrácenina slova robot, jež vyjadřuje podstatu tohoto agenta. Svým způsobem to není škodlivý software jako takový, ale dokáže znepříjemnit práci s internetem. Robot je využíván k tomu, aby vykonával sadu instrukcí, což samo o sobě není také škodlivé. Takovéto boty ale lze využít například k již zmíněným DDoS útokům, nebo k tvorbě falešných uživatelských účtů, odesílání hromadné nevyžádané pošty, známé jako SPAM, o němž bude ještě řeč.

Kontrolní otázky

Jaké známe druhy virů?
Jaký je rozdíl mezi přepisující a nepřepisující variantou souborového viru?
Vysvětlete rozdíl mezi virem a červem.
Jak probíhá DDoS útok?
Co je to botnet?

Souhrn

V této kapitole jste se naučili, jak rozpoznat jednotlivé druhy virů a červů. Bylo uvedeno, jak se vyhnout infekci. Dále byla v této kapitole zmíněna problematika botnetů a samostatných botů, jež vznikají za spolupůsobení trojských koní.

3 Ostatní škodlivý software

Cíle

Po prostudování této kapitoly:

- Získáte přehled o dalších druzích škodlivého software.
- Dozvíte se rozdíly mezi spamem a newslettery.
- Porozumíte principům spoofingu, phishingu a pharmingu.

Pojmy k zapamatování

- Malware
- Keylogger
- Spoofing
- Adware
- SPAM
- Phishing
- Spyware
- Newsletter
- Pharming

3.1 Malware

Předchozí kapitoly byly věnovány virům, trojským koňům a botnetu. Bylo řečeno, co je to a jak velké škody může napáchat na počítačích. Tento oddíl bude věnován malwaru, adwaru a keyloggerům, tedy dalšímu nežádoucímu a obtěžujícímu software.

Malware jako takový je skupina, jež zahrnuje viry, různé červy a trojské koně. Je to tedy škodlivý software, který slouží k finančnímu obohacení, nebo jako jeden z nástrojů škodlivé činnosti. Jelikož některé druhy škodlivého software již byly popsány výše, bude se tato část týkat ostatního škodlivého software, jako jsou adware, spyware, keyloggery, SPAM a další druhy nebezpečného chování. (Hoax ©2000-2015a)

V souhrnu se v případě malware v podstatě jedná o takový software, který se buď po stažení do počítače je schopen nainstalovat sám, popřípadě je nainstalován uživatelem. Poté manipuluje s vůlí uživatele ve svůj prospěch, jež zastupuje zájmy jeho tvůrce. Slouží také k obohacení, jak finančnímu, tak i informačnímu, svého tvůrce.

Obtěžování uživatele takto staženým malwarem může mít různou intenzitu. Ta svým rozsahem působí od vyskakovacích oken (=pop-up) přes různé modifikace souborů a chování systému, krádeže dat a různých hesel až po nákazu síťového rozměru. Výše jmenované skupiny mají společný prvek, kterým je možnost nákazy zejména po emailu. Útočník tak apeluje na lidskou zvědavost tím, že do nakaženého emailu umístí odkazy na různé obrázky, videa a v poslední době hlavně e-pohlednice. Při kliknutí na odkaz se ale pak uživatel dostane ke stažení nakaženého souboru, popřípadě na infikované webové stránky, jak uvádí zdroj. (Masachusets institute of technology [b.r.])

Ten se také zmiňuje o poměrně jednoduchém způsobu obrany proti škodlivému software. Na prvním místě je využívání zdravého rozumu, kterým uživatel dokáže odfiltrovat množství škodlivých stránek a nežádoucích emailů. Dalšími, z hlediska obrany dat, důležitějšími nástroji jsou aktualizovaný antivirový program, popřípadě i využití antispamového filtru. O aktualizacích software pojednává jedna z dalších kapitol. (Hoax ©2000-2015a)

3.1.1 Adware

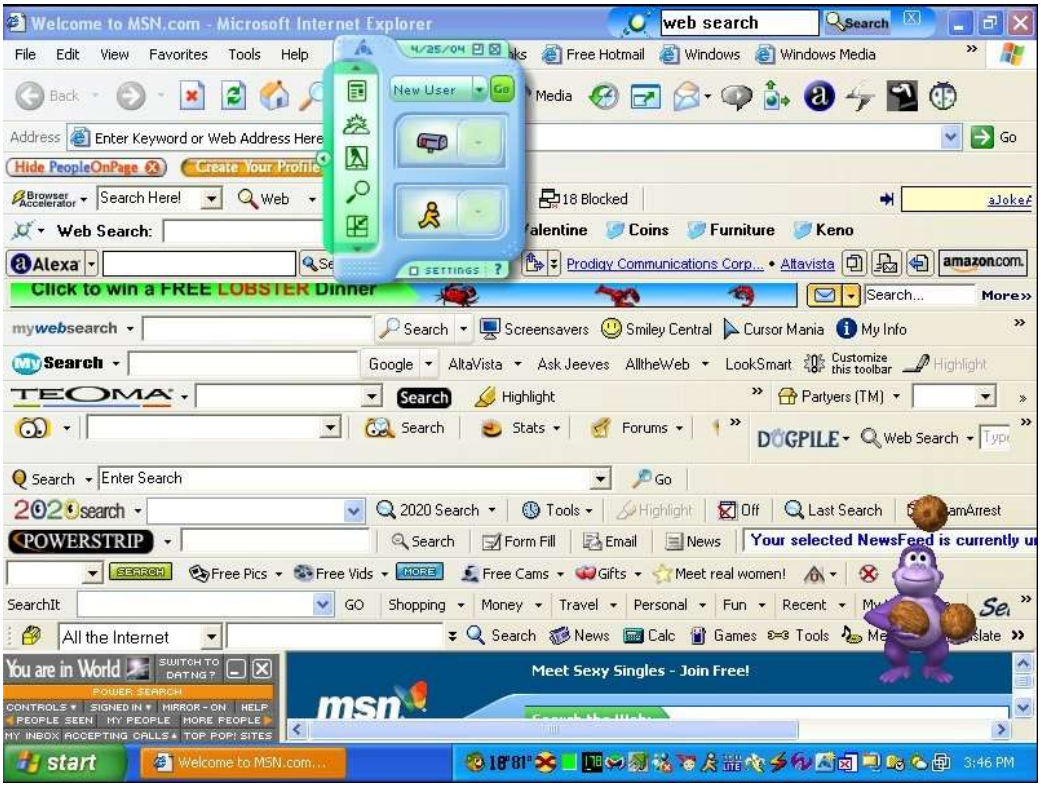
Jedním ze druhů malware je takzvaný adware. Jak napovídá název, jedná se o software sloužící k zobrazování reklamy. Toto své počínání realizuje několika způsoby, které se samozřejmě mohou vzájemně doplňovat.

Zdroj uvádí následující čtyři činnosti, které adware vykonává (PCrisk ©2015):

- modifikuje nastavení webového prohlížeče;
- zobrazuje pop-up okna;
- monitoruje činnost uživatele;
- ukládá data o návštěvě a počínání uživatele na webových stránkách.

Takzvané **modifikátory prohlížečů** umí měnit některé z uživatelsky upravitelných nastavení. Je to zejména změna domovské stránky, která jde ruku v ruce se změnou vyhledávajících nástrojů, popřípadě panelů nástrojů. Tento problém vzniká při instalaci aplikace, kdy je ponecháno zatržení různých dodatečných možností, které nemají vliv na funkci samotné aplikace. (Masachusets institute of technology [b.r.])

Obrázek ukazuje extrém, ke kterému ale může neopatrným zacházením při instalaci docházet. V prohlížeči je nainstalováno množství vyhledávacích panelů, které uživatel ke své práci nevyužije. Na surfování po webových stránkách má pak malou plochu vpravo dole (pod opičkou), kde je zobrazena stránka, na kterou byl přesměrován. Práce v prohlížeči je téměř znemožněna, variantou bývá různě velké zpomalení webového prohlížeče, jak uvádí zdroj. (PCrisk ©2015)



Obrázek 2 – Prohlížeč a adware

Zdroj: <http://thousand-tips.blogspot.cz/2014/03/easy-way-to-remove-askcom-conduit.html>

Obtěžující variantou k modifikátoru prohlížeče je vyskakovací okno s reklamou, jak je vidět na dalším obrázku. Opět jde o extrémní situaci, ne ale nereálnou. Na obrázku je navíc viditelné, že jedno z oken nabízí stažení dalšího, pravděpodobně obtěžujícího, software. Vyskakovací okna poskytují uživateli nekomfort v tom, že je nutné je zavírat a mohou zpomalovat práci s počítačem, navíc mohou být ukazatelem toho, že v systému je další z druhů škodlivého software.

Počítač může být infikován několika cestami. Adware bývá, jak již bylo uvedeno, jednou z doplňujících komponent volně dostupného software, pak také stahovacích klientů, popřípadě online instalátorů. Při instalaci software do počítače je tedy lepší kliknout na políčko "Vlastní", někde také jako "Rozšířené". Dalším krokem je zrušit zatržení u položky instalace add-on, doplňků, vyhledávačů a nastavení domovských stránek. (PCrisk ©2015)

Obrázek 3 – Ukázka zahlcení vyskakovacími okny

Zdroj: <https://threatpost.com/microsoft-to-block-unwanted-adware-july-1/105256>

Monitoring činnosti uživatelů spočívá ve sledování nákupních zvyků a vyhledávání. Toho lze pak využít při nabízení reklamních emailů a banerů, které se uživateli zobrazují, popřípadě reklamních emailů. Toto počínání není samo o sobě tolik škodlivé jako obtěžující.

3.1.2 Spyware

Monitoringem a sledováním uživatelů se zabývá také spyware, který je na tuto činnost přímo zaměřen. Pokud se uživatel připojuje na internet prostřednictvím nakaženého počítače, je veškerá jeho aktivita monitorována. Data o této aktivitě jsou pak ukládána a odesílána různým internetovým reklamním agentům. Ti je pak vyhodnocují a zasílají přímo cílenou, často obtěžující, reklamu nakaženým uživatelům, jak uvádí zdroj. (Webopedia ©2015)

Další funkcí spyware je dle zdroje také sledování emailových kontaktů, hesel k různým uživatelským účtům, anebo čísel platebních karet, prostřednictvím kterých uživatel na internetu platí. Autor spyware může rovněž obdržet soupis veškerého obsahu na disku oběti a opis každého úderu do klávesnice. Tento škodlivý software rovněž umí měnit nastavení cookies, o nichž bude ještě řeč. Spyware je tvořen souborem se škodlivým kódem, nepotřebuje tedy hostitele, jako je tomu u viru. Je to tedy jeden z červů. Nakazit se lze vzájemným sdílením a stahováním dat na P2P sítích. (Webopedia ©2015)

3.1.3 Keylogger

Keyloggery jsou ve své podstatě také druhem spyware. Jak napovídá název, mohou skenovat a uchovávat informace o každém úhozu na klávesnici. Pak tato data zasílají na předem určenou adresu. Autor keyloggeru tak může obdržet jakékoliv citlivé údaje a data, která může využít k další škodlivé činnosti. Příkladem je zcizení internetové identity a přístup do profilů nejen na webu. Navíc, pokud se jedná o pokročilou verzi škodlivého software, získá útočník jako na stříbrném podnose informace o navštívených stránkách a kontaktech prostřednictvím emailových adres, které keylogger zaznamenal. Zpravidla se tento druh sledování využívá v korporátní sféře, kdy zaměstnavatel zjišťuje, jak zaměstnanci rozkládají čas a práci na počítači mezi skutečně odpracovaný výkon a mezi volnočasovou aktivitu na internetu. (Webopedia ©2015)

Další ze zdrojů definuje keyloggery následovně. *"Keylogging, jak je tento útok odborně nazýván, může mít hardwarovou i softwarovou podobu. Botnety využívají logicky softwarovou variantu, díky níž mají přehled o všech stisknutých klávesách napadeného počítače. Získání přístupových hesel je pak pro útočníky otázkou okamžiku."* (Klubal 2013, s. 16)

Oba zdroje se tedy shodují na tom, že ve špatných rukách jde o velice nebezpečný nástroj, jehož prostřednictvím může dojít i ke ztrátám finančním. Například přihlášení do internetového bankovnictví některých institucí totiž probíhá zadáním číselných kódů, což představuje zranitelnou část. Proto je přístup jištěn pomocí zabezpečeného protokolu SSL a informační textové zprávy s kódem, který je nutné zadat.

3.1.4 SPAM vs. Newsletter

SPAM je určitý druh nevyžádané emailové zprávy s reklamním sdělením. Svým obsahem uživatele obtěžuje a krade mu drahocenný čas. Zpravidla je tato reklama zasílána na emailové adresy v celé databázi. Nerozděluje příjemce na skupiny dle věku, pohlaví, nebo osobních preferencí. Typicky má podobu nabídky léků volně neprodejných, nebo prodejných s omezením, popřípadě zázračných přípravků. Patří sem ale i různé výhry od podivných společností, nebo finanční převody a dědictví. Ve všech případech jde o to, aby se tvůrce této nechtěné reklamy obohatil na úkor neznalého uživatele.

Do příjmu spamů se lze zapsat několika cestami. První z nich je otevírání již přijatých spamů, které mohou obsahovat odkazy na další škodlivý kód, nebo dokonce některý malware v příloze. Další z možností, jak se nakazit, představuje přílišné zadávání a zveřejňování emailové adresy na internetových diskuzích. Spam také posílají boti, kteří zároveň vyhledávají emailové adresy na zmíněných diskuzích, pomocí textových zpráv na mobilní telefony a na chatu, kde je možné obtěžující chování hlásit a administrátor tak spamera odpojí z diskuze, nebo od internetu. Nakažený uživatel může být někdy sám spamerem. Bývá tomu tak, pokud má zavirovaný počítač a stal se takzvaným botem. Útočník tak může řídit jeho aktivitu a odesílat z jeho počítače spamy, aniž o tom nakažený uživatel ví, jak uvádí zdroj. (Bezpečný internet [b.r.])

Boti si také umí sami generovat emailové adresy. Vymýšlí část danou před zavináčem o určité délce, k níž přidají zavináč a některou ze známých domén. Toto počínání má sice za následek spoustu nepoužitých emailových adres, ale botům to nijak nevadí, jak uvádí zdroj. (Horák 2006)

Příkladem spamu je následující obrázek, který je jasně rozpoznatelný. Nejde v něm o klasický přátelský email, ale jasně vykazuje znaky obtěžování. Prvním z vodítek může být špatný pravopis, slovosled ve větách a špatné použití českého jazyka vůbec. Tyto chyby vznikají při použití strojového překladu, tedy prováděného přes různé překladače, které nemají tak vyvinutý jazykový cit jako rodilý mluvčí popřípadě jako člověk zvyklý jazyk využívat pravidelně.

Dalším znakem může být několikajazyčná mutace. Ta ukazuje na to, že u emailu není rozlišeno, komu bude doručen. Ani jeden příjemce nemusí znamenat, že email byl zaslán pouze tomuto. Vzpomeňme si na využití skryté kopie při rozesílání emailů. Opět zde platí, že jde o dobrý nástroj při správném použití, je ale špatným pánem.

Obrázek 4: SPAM

Zdroj: <http://www.bezpecnyinternet.cz/zacatecnik/e-mail/spam.aspx>

Spam je škodlivý z několika důvodů. Při nadměrném množství snižuje volnou kapacitu v emailové chránce. Dále také zatěžuje servery a je příčinou prodlev. Z časového hlediska se uplatňuje i u uživatele, kterému trvá delší dobu rozlišit, zda jde o vyžádaný, nebo nevyžádaný email. Z hlediska finančního se jedná o zátěž pro obě dvě strany. Provozovatel poštovního serveru má náklady na detekci a štítkování pošty a uživatel, kterému déle trvá poštu rozlišit, má pak náklady v případě placeného připojení k internetu. Také může docházet k tomu, že je smazán důležitý email, popřípadě zařazen mezi spamy a uživatel ho tak přehlédne, jak uvádí zdroj. (Horák 2006)

Oproti spamu ještě existuje vyžádané reklamní sdělení, kterému říkáme newsletter. Je obvykle zasíláno od obchodníků, od nichž uživatel nakoupil zboží, popřípadě se u nich registroval a dal svolení k zasílání těchto obchodních sdělení. Z takového registrace se lze vyvázat, jak ukazuje obrázek.

Na obrázku je viditelný běžný newsletter, k jehož odběru se uživatel zaváže při registraci. Z odběru newsletterů se lze odhlásit kliknutím na odkaz Odhlásit Newsletter na konci emailu (na obrázku vpravo dole). V tomto případě je uživatel skutečně odhlášen z odběru a již mu nechodí reklamní nabídky.


Výdej jen v obvykle běžném množství. Nabídka jen do vyprodání zásob. Změny vyhrazeny. Zobrazené artikly jsou příkladem pro dostupné barvy a modely. Prosíme, abyste omluvili barevné odlišnosti, zpoždění dodávky a chyby v cenách.

Stát se fanouškem:

Vaše zákaznické číslo: [redacted]

Právě jste obdržel(a) mail, který potvrzuje vaše úspěšné přihlášení do VIP-servisu Takko Fashion. Tento servis je zdarma. Děkujeme vám za vaši důvěru a závazně přebíráme odpovědnost za ochranu vašich osobních údajů.

Znamená to, že vámi sdělené údaje nebudou předány žádné třetí osobě!

Takko Fashion s.r.o.
Čechyňská 365/23
602 00 Brno
Česká republika
E-Mail: service_cz@takko-fashion.com

Takko Fashion s.r.o.
Oddíl: C
Vložka: 46900
jednatelé: Alexander Mattschull, Hannes Rumer, Andreas Silbernagel, Paul Thieme, Andreas Kromer

Pokud si nepřejete dostávat od nás žádné informace ve formě Newsletteru, klikněte prosím na tento odkaz: Odhlásit Newsletter

Obrázek 5 – Newsletter

Zdroj: převzato z emailové schránky autorky

Problematické bývá, pokud neznalý uživatel, kterému přišel spam, objeví v dolní části odkaz na odhlášení z odběru spamů. Pokud jde o podvrh, zapíše se tak k odběru dalších spamů, jak uvádí zdroj. (Bezpečný internet [b.r.])

3.2 Další druhy nebezpečných útoků

3.2.1 Spoofing

Spoofing je další z druhů klamavého jednání, kdy se útočník vydává za jiného uživatele. Význam anglického slovesa to spoof je podobný slovu to fool, znamená klamat. Zahrnuje v sobě způsoby, jak získat na internetu identitu někoho jiného. Funguje na poli URL adres, emailů, krátkých textových zpráv, IP adres a dalších.

Jeden ze druhů spoofingu je takzvaný email spoofing, jehož princip byl zmíněn v kapitole o spamech. V tomto případě hacker nahrazuje svou emailovou adresu emailovou adresou jiného uživatele. Maskuje se tedy, aby nemohl být odhalen, a využívá identitu jiného uživatele. V případě odhalení ukazují totiž stopy na osobu, jejíž email byl infikován. Podobně vypadá i takzvaný SMS spoofing, jak se zmiňuje zdroj. (IT slovník ©2008-2015)

Dalším ze druhů je IP spoofing. Každý počítač v počítačové síti má přidělenou takzvanou IP adresu. Tuto adresu může mít buď každý počítač stále stejnou, nebo je přidělována podle toho, který počítač se připojí do sítě dříve. Problematiku rozdělování IP adres v síti řeší takzvané DHCP servery a lze o ní dohledat více na internetu. IP spoofing spočívá tedy v tom, že hacker pomocí některého škodlivého software najde IP adresu, která má povolen přístup do sítě, popřípadě do systémů, jež jsou v okruhu zájmů další osoby. Když nalezne správnou IP adresu, zamění ji za svou skutečnou v paketech, které vysílá směrem k serveru. Pakety obsahují data, která jsou zabalena a je k nim dosazena hlavička. Obsahem této hlavičky jsou právě informace o IP adresách a další. (Webopedia ©2015)

Další ze zdrojů se zmiňuje o pozitivním využití IP spoofingu v síti. Provoz v počítačové síti je mimo jiné založen na zasílání kontrolních paketů, kterými se tato síť monitoruje. Routery, místo aby přeposílaly tyto pakety po síti, tak maskují svou IP adresu a posílají zpět pakety za jiná zařízení. Tím se zmenšuje zatížení sítě a zvyšuje její propustnost. Není tedy tolik zatížena. (Webopedia ©2015)

3.2.2 Skryté sledování

V kapitole o škodlivém softwaru bylo zmíněno, že zaměstnavatel sleduje aktivitu svých zaměstnanců. Je to jeden ze způsobů skrytého sledování, jinými slovy ratting. Pojmenování vychází z názvu nástrojů pro vzdálenou správu, anglicky Remote Access. Za tímto aktem stojí jeden z trojských koňů (Remote Access Trojan), který slouží k provádění špiónské činnosti a výše zmíněnému sledování. (Get safe online ©2015)

Uživatel si může infikovat počítač opět buď emailem, nebo stažením nějaké hry z neprověřených stránek. Běžným způsobem je neodhalitelný, neboť jeho aktivita není nápadná. V seznamu úloh není zobrazován, systém si myslí, že je to jeho interní program. Výkon stroje také výrazně nezmenšuje, jak je uvedeno ve zdroji.

Zmiňuje se o těchto rizicích (Get safe online ©2015):

- fyzické sledování;
- monitorování aktivity;
- zapojení do botnetu;
- popřípadě ztráta dat.

Fyzické sledování probíhá po webkameře, ovšem daleko nebezpečnější je nahrávání aktivity v domě a vybrané osoby, popřípadě sdílení těchto nahrávek po internetu. Uživatel toto běžně není schopen zjistit, jelikož se nezapíná kontrolní dioda u webkamery, popřípadě jiného zařízení. Monitorování spočívá v ukládání, uchovávání a šíření záznamů jako v případě keyloggerů. Hacker tedy může získat veškeré informace o identitě napadnutého uživatele. Poslední možnost znamená: smazání, nebo modifikace dat a různé modifikace souborového systému. (Get safe online ©2015)

Rattingu se lze vyhnout opět využíváním aktualizovaného antivirového systému, popřípadě doplnění formou antispywarového systému a firewallu, o němž bude dále ještě řeč. Dále pak využitím jen souborů z ověřených zdrojů, čímž je vyloučeno sdílení souborů v P2P sítích. V případě ochrany platí již zmíněné v oblasti škodlivého software. (Get safe online ©2015)

3.2.3 Phishing a pharming

Při rhybaření, jak je jinak phishing nazýván, jde o získávání přihlašovacích údajů k účelům obohacení se z konta postižených tímto chováním. Jinými slovy se jedná o vylákání přihlašovacích údajů, hesel a podobných informací, popřípadě přímo zadání těchto a zaslání peněz na účet útočníka. V loňském roce se rozmohl počet těchto útoků, které byly zaměřené na důvěřivé klienty některých bankovních a finančních ústavů.

Phishing je útok, který lze při troše přemýšlení odhalit, čímž se mu lze vyhnout. Většinou dostane "postižený" nevyžádaný email, kde je vyzván k zadání přihlašovacích údajů z důvodu různých ověření a podobných. Již v tomto kroku by měla uživateli začít v hlavě svítit červená kontrolka, neboť je nepravděpodobné, že by finanční ústavy rozesílaly zprávy takové povahy pomocí zpráv elektronické pošty. Druhým krokem kontroly může být emailová adresa, ze které je odeslána zpráva, popřípadě lze zkontrolovat pravopis, který je použit při jejím psaní. Většinou jde totiž o strojově přeložený text z některého z cizích jazyků a takové počínání je na něm zřetelně znát. Pokud ani tento krok nevede k odhalení podvodného emailu, lze ještě při kliknutí na odkaz zkontrolovat adresu, kde se web nachází. V případě pochybností má každá peněžní instituce na svém originálním webu telefon na infolinku, nebo kontakt na technickou podporu, s jejíž pomocí lze dohledat, zdali bankovní dům tento email poslal, navíc pro komunikaci s uživateli banka používá jiné kanály, například zprávy zasílané pomocí aplikace internetového bankovnictví, kde finanční ústavy zasílají varování, aby uživatelé neotevírali podvodné emaily podepsané jejich jmény, popřípadě neklikali na odkazy a nezadávali žádné přihlašovací údaje. Pokud je problém, obvykle se ozývá osobní bankéř a sjednává si s klienty schůzku, aby je řešil osobně. V případě phishingových útoků sehrála velkou roli i média, která podrobně informovala o možnosti obdržení těchto nevyžádaných emailů. Pokud přesto uživatel neodhalí tento podvodný email je nutné při zadání údajů a zobrazení hlášky o odejití platby zavolat neprodleně na klientskou linku banky a toto řešit. Je mi znám případ, kdy klientka České spořitelny toto z různých důvodů neodhalila a protože ihned kontaktovala klientskou linku, došlo k zablokování odcházející platby a problém byl vyřešen poměrně klidně.

Jak uvádí zdroj, phishingový útok probíhá tak, že emailem obvykle finanční instituce žádá o zadávání osobních údajů do různých webových formulářů. Z adresy webu je navíc znatelné, že nepoužívá zabezpečený protokol, který bankovní instituce vždy používají. Obrana může být opět tvořena víceúrovňově. Základ tvoří aktualizovaný software v počítači. Dalším prvkem je neotevírat podivné emaily. Naprostou samozřejmost představuje práce na zabezpečeném a nesdíleném počítači, v případě sdílení v jedné domácnosti doporučujeme nastavovat každému jeho účet bez administrátorských práv. Pak je pod kontrolou instalace nového software. Pokud se uživatel chce přihlásit do internetového bankovnictví, je lepší URL adresu zadat ručně a zkontrolovat překlepy. Minimalizuje se tím možnost, že bude uživatel přesměrován na nějaký z nebezpečných webů. Pokud se aplikace chová nestandardně, nebo je třeba zadat nějaké zvláštní údaje, je lepší ji ihned ukončit a uvědomit o tom neprodleně svou banku. (Hoax ©2000-2015b)

Vedle phishingu existuje útok také zaměřený na aplikace internetového bankovnictví, tentokráte se jmenuje pharming. Jak uvádí zdroj, je v pozadí webu skript, který zařizuje přesměrování uživatele po přihlášení do aplikace internetového bankovnictví na některý ze škodlivých webů. Takovéto chování jde identifikovat mimo jiné také tím, že se aplikace nechová standardním způsobem, popřípadě chce zadat i jiné než přihlašovací údaje. V tomto případě zdroj radí okamžité odhlášení od podivné aplikace a oznámení této skutečnosti technické podpoře dané aplikace. (Bezpečný internet [b.r.])

Kontrolní otázky

Vysvětlete, jaké skupiny software zahrnuje malware.
Jmenujte hlavní rozdíly mezi adware a spyware.
Popište princip útoku prováděného keyloggerem.
Jaký je rozdíl mezi spamem a newsletterem?
Jaký je rozdíl mezi phishingovým a pharmingovým útokem?

Souhrn

Prostudováním této kapitoly jste získali přehled o dalších druzích škodlivého software, jako jsou zejména malware, adware a keyloggery. Zároveň jste poznali principy nebezpečných útoků, kterými jsou sledování přes webkameru, pharming a phishing. Již umíte tyto útoky rozpoznat a vyvarovat se jim.

Literatura a zajímavé odkazy

Bojem s kyberkriminalitou se zabývá web http://www.antiphishing.org

4 Hackeři

Cíle

Po prostudování této kapitoly:

- Budete umět vysvětlit rozdíl mezi hackery a crackery.
- Naučíte se je rozlišovat dle různých kritérií.
- Budete umět vysvětlit, kdo je hacker a co je motivem jeho činnosti.

Pojmy k zapamatování

- Hacker
- Black hat
- Wizard
- Cracker
- Grey hat
- White hat
- Guru

4.1 Úvod

Jako hackeři jsou dnes označováni uživatelé počítačů, kteří se snaží využívat všech prostředků k získání identity, citlivých údajů, popřípadě přihlašovacích údajů k různým systémům, například internetovému bankovnictví, nebo třeba zdravotní kartě, ale i různým herním systémům. Původ tohoto slova ale není tak jednoznačný, jak by se mohlo na první pohled zdát. Původně totiž slovo hacker neznamenalo žádné hanlivé označení. Byl to výraz pro odborníka ve svém oboru, který toto demonstroval přístupem do různých systémů.

Zdroj definuje hackera jako člověka, který je schopen vstoupit do zabezpečeného systému, čímž prokazuje své odborné kvality. Tím ovšem jeho počínání v tomto systému končí, hacker jako takový se nesnaží získat z tohoto systému data, ani se nesnaží je nijak poškozovat. Svoje počínání bere spíše jako hobby nebo sport, který je ovšem velmi časově náročný. Pokud získá nějaký program, tak jen pro sebe a úzký okruh přátel. Hacker obecně nezískává software pro finanční obohacení. Hacker v kyberprostoru je jedinec s velice velkým okruhem technických znalostí. Zdroj dále uvádí, že je to člověk velice kreativní, který pro svou potěchu programuje rychle, nehodlá se totiž zabývat vyřešením jednoho problému dlouhou dobu, a dělá to tak, aby jeho kód nebyl tak snadno čitelný pro ostatní, což obnáší i to, že se nezatěžuje tvorbou dokumentace a komentářů, jelikož pro něho je jeho vlastní kód čitelný. (Jirovský 2007, s. 51)

Pro hackera je hlavním motivem, aby se stal uznávaným mezi odbornou komunitou. Uznává tedy odborníky v oboru jako autority, jejichž práce je hodna toho, aby se o ni zajímal. Mocenské autority přehlíží. Dále má na mysli svobodu jedince a svobodný přístup k informacím. Cítí se morálně zavázán ke sdílení informací s ostatními v komunitě a také se dělí o své know-how, z čehož vyplývá, že se snaží hlavně si budovat dobré jméno, chce být oslavován pro své technologie a technické dovednosti. Mezi principy hackingu tedy patří tvoření open-source kódů, aby kdokoliv tyto programy mohl zdokonalovat, popřípadě je vyladit k dokonalosti. (Jirovský 2007, s. 52)

Když se hacker dostane do systému, nesnaží se nějak ničit data, popřípadě snižovat jejich stupeň utajení. Pouze si odškrtne cíl a dá vědět administrátorovi o tom, proč se do systému naboural a jak toho dosáhl. Samozřejmě tak činí způsobem, aby nebyl odhalitelný. Většinou se snaží i navrhnout řešení, jak tuto díru v zabezpečení odstranit. (Jirovský 2007, s. 52-53)

4.2 Hackerská etika

Většina hackerů se shoduje na uznávání hackerské etiky, která má dle zdroje osm bodů. Jsou to tyto (Jirovský 2007, s. 53):

"1. Přístup k počítačové technologii je pro všechny bez rozdílu a zdarma.

2. Všechny informace zdarma.

3. Nedůvěřujeme vládě a obecně mocenským autoritám, podporujeme decentralizaci.

4. Hackeři mají být posuzováni podle jejich dovedností jinými hackery a ne nějakou formální organizací nebo jinými nerelevantními kritérii.

5. Na počítači je možné vytvořit i umění a krásu.

6. Počítače mohou změnit život k lepšímu.

7. Hacker nikdy nepoškodí systém.

8. Hacker se nikdy neprolamuje do státních počítačů."

4.3 Osobnost hackera

Hackeři si, jako u každé jiné komunity, také vymysleli vlastní způsob dorozumívání, který vyplývá z technologií, jež využívají. Baví se spolu jazykem plným specifických technických výrazů, písemnou komunikaci pak rovněž upravují. Jejich humor by se někomu mohl zdát prázdný, ale není tomu tak. Stejně jako u jazyka využívá pouze znalosti z oboru a vhodně je upravuje, jak opět uvádí zdroj. (53-54)

Následující tabulka dělí hackery na několik typů podle různých kritérií.

Kritérium	**Skupina**
Aktivita	· hackeři; · crackeři
Kloboukové dělení	· White hats; · Black hats; · Grey hats
Brilantní programátor	· Guru; · Wizard

Tabulka 2 – Rozdělení hackerů dle různých hledisek

Zdroj:(54,55), upraveno

První kategorie rozděluje hackery dle aktivity prováděné na síti na **hackery**, kteří se snaží pomáhat, a **crackery**, kteří na internetu provádějí záškodnickou činnost. Hlavním důvodem práce crackerů je osobní zisk, popřípadě podpora různých extrémistických skupin a další nelegální činnost. (Jirovský 2007, s. 54)

Takzvané "Kloboukové dělení" využívá princip rozdělení na hodné a zlé dle westernových příběhů. Znamená to tedy od bílé, až po černou. Takzvaní **White hats** představují to dobré. To tedy znamená, že uznávají zejména hackerskou etiku a morální principy. Zpravidla se nechávají zaměstnávat jako testeři bezpečnosti systémů. Svými triky se snaží obalamutit systém a hledají slabiny a zranitelná místa. (Jirovský 2007, s. 54)

Black hats jsou jejich pravým opakem. Odhodily stranou veškerou morálku a etiku a věnují se hlavně zisku. Také se snaží prolomit veškerou ochranu, ne ale kvůli bezpečnostní analýze jako v předchozím případě, ale kvůli získání výhod, popřípadě přímo špionáži konkurenčních technologií. Pokud se jim nedaří systém konkurence prolomit a dostat se do něho, tak tam bývají zaměstnáváni a odesílají důvěrná a citlivá data tomu, kdo je najal. (Jirovský 2007, s. 55)

Grey hats potom představují hackery, kteří mají stejné znalosti a zkušenosti jako obě předchozí skupiny, ale ještě nevědí, na kterou stranu se přidat, respektive nejsou si stoprocentně jistí, která barva jim bude vyhovovat jako z hlediska zisku, tak z hlediska morálního. (Jirovský 2007, s. 55)

Poslední kategorií dělení jsou takzvaní "Brilantní programátoři", jak uvádí zdroj. Jde o velice plodné hackery, co se tvorby kódu týče. Programují si ale spíše sami pro sebe, jelikož se nezatěžují tvořením dokumentace, popřípadě alespoň komentováním kódu. Když mají nějaký problém, snaží se přizpůsobit program, tak aby jim vyhovoval. Z uvedeného vyplývá, že jde spíše o samostatné pracovníky, než o týmové hráče. I tito se dále dělí na dvě skupiny: Guru a Wizardy. **Guru** je zkušený člověk, který má spíš povrchnější znalosti, ale umí je aplikovat na širokou škálu problémů se stoprocentním řešením. Oproti tomu **Wizard** sice do detailu zná problém a jeho stavy a také ho dokáže vyřešit, ale jeho řešení nefunguje v krajních stavech problému. Navíc je nepochopitelné pro ostatní programátory. (Jirovský 2007, s. 55)

Následuje shrnutí uvedených skupin. Pro zisk dělají svou činnost crackeři. Profesionálně se hackování zabývají kloboukoví hrdinové. Neuspokojení zaměstnanci provádějí záškodnickou činnost s jediným cílem, a to nějakým způsobem uškodit svému zaměstnavateli. Další skupinu tvoří ideologisté, kteří jsou spjati s nějakou událostí, snaží se na ni upozornit a prosazovat své názory z hlediska politiky a, jak napovídá název, ideálů a cílů. Script-kiddies mají oproti ostatním skupinám malé znalosti, ale zato obrovské cíle. Nedokáží plně docenit správnou aplikaci a do řešení problému se vrhnou po hlavě. Snaží se bez předem dané strategie využívat cizího kódu a touží po maximální slávě. Poslední skupina vychází ze script-kiddies a tvoří ji dospělí, jež neuspěli v oboru a stále touží po slávě. (Jirovský 2007, s. 56)

Kontrolní otázky

Jaký je rozdíl mezi hackerem a crackerem?
Kdo je to guru?
Jaké jsou principy hackerské etiky?
Proč vznikají script-kiddies?

Souhrn

Prostudováním této kapitoly jste získali představu o tom, co hackery a crackery motivuje. Také již umíte tyto pojmy od sebe odlišit. Dozvěděli jste se, že ne všichni hackeři provádějí různé výše popsané útoky, aby se obohatili.

5 Ochrana proti škodlivému software

Cíle

Po prostudování této kapitoly:

- Získáte přehled o funkci ochranného software.
- Nastudujete rozdíly mezi antivirem a firewallem.
- Dozvíte se, jak probíhají antivirové kontroly.

Pojmy k zapamatování

- Antivir
- Virová databáze
- Rezidentní štít
- Sandbox
- Karanténa
- Test integrity
- Whitelist
- Heuristická analýza
- Firewall

5.1 Antivir

Ochrana proti škodlivému software existuje několikastupňová s tím, že čím více ochranných prostředků uživatel využívá, tím menší je šance, že bude jeho počítač infikován. Domnívám se, že nejznámější druh ochrany představuje antivirový program. Dnes je na trhu velké množství těchto antivirů. Základní ochranu, testování počítače a automatické aktualizace lze pořídit zdarma. Placené jsou většinou další rozšiřující možnosti ochrany, jako je ochrana dat, osobních údajů, zabezpečení při nakupování a využívání online bankovnictví, blokace podvodných emailů a spamů, ale také oficiální technická podpora od výrobce.

Antivirový program se snaží monitorovat dění zejména na vstupních a výstupních portech a nabízí různé další komponenty než jen srovnání s virovou databází. O nástrojích antivirových systémů bude psáno v dalších částech.

A dělí se dle zdroje na tři skupiny (Antivirové centrum ©1998-2015):

- On-demand antiviry;
- Jednoúčelové antiviry;
- Antivirové systémy.

První skupinu tvoří takzvané **antiviry na vyžádání**. Ty se používají zejména, pokud je počítač nakažený tak, že není schopen nastartovat klasickým způsobem operační systém. Pak lze spustit operační systém DOS a v něm provést protizáškodnické aktivity pomocí on-demand antiviru. Jak napovídá název u druhé skupiny, **jednoúčelové** antiviry jsou využívány zejména k odstranění akutní široce rozšířené nákazy. (Antivirové centrum ©1998-2015)

Nejrozšířenější skupinu potom tvoří takzvané **antivirové systémy**. Ta představují kompletní zabezpečovací řešení, které chrání před všemi druhy škodlivého software, elektronickou poštu a nabízí další možnosti a nástroje, jak zabezpečit svá data. Jak uvádí zdroj, dostávají tyto systémy pravidelně aktualizované virové databáze, což samozřejmě pomáhá zlepšovat nalezení škodlivého software. (Antivirové centrum ©1998-2015)

Z uvedeného vyplývá, že nejvíce využívanou skupinou jsou antivirové systémy. Tyto tedy nabízí možnost nejen ochrany před viry, ale i hledání škodlivého kódu a aktivní práci se škodlivým souborem, k tomu využívají několika metod. Mohou kontrolovat konkrétní soubory na vyměnitelných úložištích a pevném disku, pokud to zrovna uživatel potřebuje. Dále mohou využívat **metodu nebezpečného chování.** Ta spočívá v tom, že antivirus sleduje aktivity programů, které se týkají práce se spustitelnými soubory, například zápis a modifikaci. Pokud toto antivirový program vyhodnotí za nepřípustné, dá echo uživateli. I když tu může být jisté procento špatně vyhodnocených případů, je spíše větší pravděpodobnost, že se podaří odhalit škodlivý software, který ještě není zadán do antivirové databáze. (Binnary ©2012)

Sandbox je rozhraní, které umožňuje nasimulovat funkci neznámého souboru. Je to vlastně tedy simulátor, ve kterém lze spustit jakýkoliv software, aniž by byl nakažen počítač. Výše již bylo uvedeno, že může docházet k chybným detekcím ze strany antivirového programu, v sandboxu lze zkontrolovat funkci tohoto souboru. Pokud je v pořádku, lze ignorovat aktivitu antiviru proti tomuto souboru. Pokud dojde k záškodnické činnosti v sandboxu, není tím automaticky nakažen počítač uživatele testujícího soubor, jak uvedl zdroj. (Binnary ©2012)

Stává se, že kontrola, zvláště pevného disku, trvá delší dobu, než by bylo žádoucí. Tvůrci antivirového software proto vyvinuli takzvaný **whitelist**, do kterého antivirus umístí soubory určité soubory. Pokud jsou tyto soubory bez jakékoliv modifikace, nemusí je již kontrolovat při příštím skenování. (Binnary ©2012)

Aby mohl antivirus efektivně pracovat, musí mít aktualizovanou virovou databázi. **Virová databáze** v sobě obsahuje určité celky kódů škodlivého software, se kterými antivirový software porovnává skenované soubory. Tuto databázi je pak nutné aktualizovat pokaždé, když vyjde nová verze, což se děje zpravidla denně. Aktualizace jednou za čas není efektivní. (Binnary ©2012)

Antivirový systém pak nabízí možnost léčení, popřípadě opravy takového souboru, jeho umístění do karantény, nebo přímo smazání. **Vyléčení** spočívá ve vymazání sekvence škodlivého kódu ze souboru. **Karanténa**, jak napovídá název, slouží k selekci celého souboru a znemožnění tomuto jakékoliv další činnosti a tím i rozvoji, popřípadě další nákaze. Pokud uživatel není schopen vybrat ani jednu z možností, popřípadě otestovat soubor v sandboxu, aby se mohl efektivně rozhodnout, je logickým vyústěním smazání souboru. Je nutné mít na mysli, že rozhodnutí uživatele má dopad na celý systém, nebo i další počítače v síti. (Binnary ©2012)

Neméně důležitým pojmem v oblasti antivirů je **heuristická analýza**. Při té dochází k monitorování činností souborů. Nastavujeme i ní citlivost, jejíž vhodnou míru je nutné zvážit. Pokud je míra na nízké úrovni, může docházet k ignorování činnosti některého škodlivého software. Když je naopak moc vysoká, tak dochází k falešným poplachům, které zdržují od práce uživatele. Z uvedeného vyplývá, že obě možnosti představují špatnou volbu. Nástroje heuristické analýzy smí přistupovat nejen k souborům vytvořeným uživatelem na disku, ale i do systémových souborů a spouštěcích oblastí, a smí tak monitorovat jejich činnost. (Bitto 2011)

Rezidentním štítem se pak rozumí sledování počítače a jeho vstupně výstupní aktivity za běhu. Tento štít může detekovat škodlivý soubor před průnikem do systému. Kontroluje tedy veškeré soubory, se kterými uživatel a operační systém pracují. (Bitto 2011)

Posledním z nástrojů, které antivirový systém využívá k ochraně dat a počítače uživatele, je **test integrity**. Tento test je založen na tom, že antivirový program si pro každý soubor vytvoří sadu informací, kde jsou zejména kontrolní součty, velikost a podobné údaje. Vypočtená data jsou potom porovnávána s daty, které si pořídí ve chvíli testování. Pokud je soubor nějakým způsobem infikován, tak se mění jeho podoba pro antivirový program. Test integrity tedy slouží k tomu, aby nalezl stopy spíše než různé probíhající infekce počítače. Stejně jako u heuristické analýzy může ale docházet k tomu, že antivir vytváří falešný poplach. To se děje z důvodu změn například po aktualizování aplikace. (Bitto 2011)

Doplňkem k nainstalovanému antiviru je možnost testování online, buď na stránkách výrobců těchto řešení, nebo souhrnným testováním. Výhodou je, že uživatel není nucen instalovat do počítače další software. Nevýhod ovšem tato možnost přináší více. Zmiňme zejména absence kontroly diskových jednotek. Slouží tedy spíše jako kontrola na vyžádání, pokud je nutné otestovat malé množství souborů. Takovou možnost představuje například služba VirusTotal, o které bude další část. (Bitto 2011)

5.1.1 VirusTotal

Jelikož se každému jednou může hodit tento doplňkový nástroj, rozhodla jsem se provést malou demonstraci služby VirusTotal, kterou přináší společnost Google jako bezplatnou online funkci. Antivirové scanery jsou schopné identifikovat veškerý škodlivý software, který byl zmíněn. Hodí se tedy i pro případ ověření souboru při falešném poplachu.

Poznámka

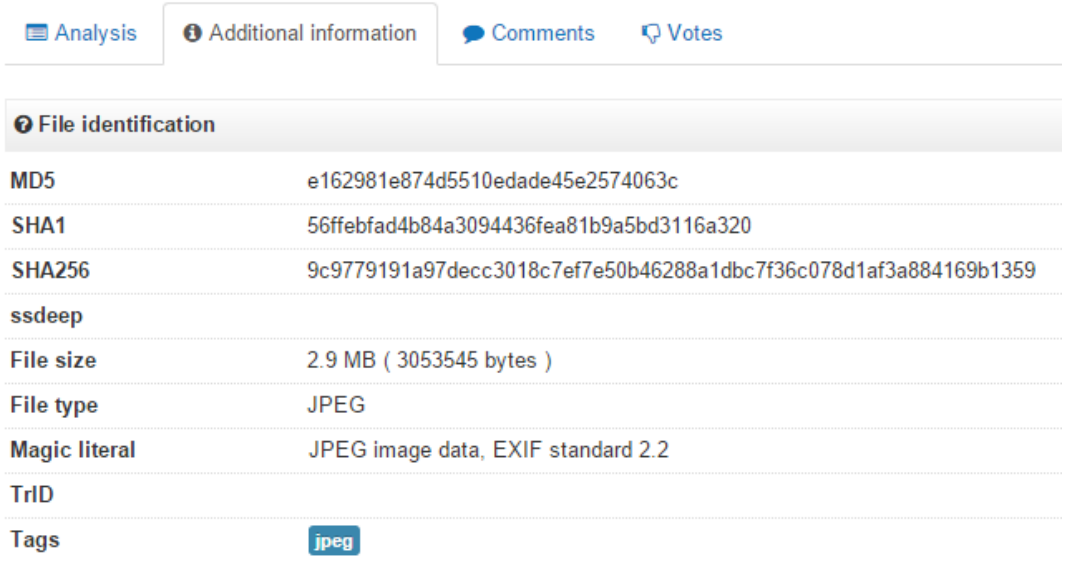
Více informací a samostatné testování lze nalézt na webových stránkách: https://www.virustotal.com

Nyní přejděme k samotné analýze. Na úvodní stránce služba nabízí testování souborů a URL. Soubory ke skenování lze vkládat do velikosti 128 MB, URL adresy potom v celém znění. Po uploadu souboru na server provede analýzu pomocí celé řady online virových skenerů od různých výrobců. Výsledek je viditelný na obrázku níže.

Obrázek 6: Výsledek analýzy vloženého souboru

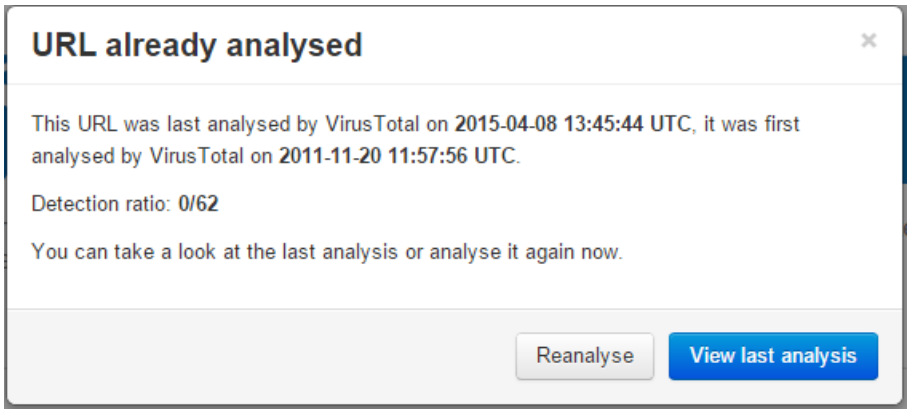
Zdroj: analýza provedená na webu autorkou

Po provedení analýzy se zobrazí základní informace a seznam webů, kde byla provedena analýza, který byl pro naše účely zkrácen. Jak je vidět na obrázku, testování se účastnilo 53 různých antivirových skenerů. Výsledek je také vidět už na první pohled v části vpravo, na pohled druhý potvrzuje číselný údaj (Detection ratio), že soubor je v pořádku. V záložce Additional information jsou pak zobrazeny dodatečné informace o souboru, jak je vidět na dalším obrázku, tedy velikost, formát a další charakteristiky.



Obrázek 7 – Dodatečné informace při analýze souboru
Zdroj: analýza provedená na webu autorkou

Podobně je to s testováním libovolné URL adresy. Je zapsána a systém provede testování. Výsledky takového testování mohou být pouze dva, jak je vidět na obrázku pod textem. Buď již bylo provedeno testování a lze zobrazit již hotovou analýzu, potom nabízí i datum, kdy analýza byla provedena a nebo lze vytvořit novou analýzu. Informace o provedené analýze jsou pro případy blízkého testování po sobě.



Obrázek 8 – Výsledek analýzy URL
Zdroj: analýza provedená na webu autorkou

Po výběru jedné z možností je provedena vyžádaná akce a jsou zobrazeny výsledky ve stejné podobě jako v případě analýzy souboru.

5.2 Firewall

Další stupeň ochrany představuje využití firewallu, který chrání uživatele zejména tím, že od sebe odděluje počítačové sítě. Funguje tedy svým způsobem jako router s doplněním o bezpečnostní kontrolu, kterou ale není radno podceňovat. Zatímco router podle svých nastavených pravidel vpustí do počítačové sítě veškeré pakety, firewall dle svých charakteristik pečlivě třídí, jaký paket do sítě za ním vpustí.

Firewall lze pořídit jak hardwarový, tak softwarový, jejichž charakteristiky budou rozebrány dále. **Hardwarový firewall** se odlišuje od softwarového tím, že bezpečnostní řešení má pro sebe vyhrazen svůj vlastní hardware, čímž může zařízení přinášet větší výkon. Na druhou stranu je omezeno pouze na poskytování bezpečnostních služeb, nenabízí tak jiné doplňkové funkce, jako v případě software nainstalovaném na serveru. Problém nastává v případě větší poruchy, jelikož je nutná také vyšší investice, jak uvádí zdroj. (Přibyl ©2010)

V případě **softwarového firewallu** je sdílen hardware s dalšími programy, které tak mohou snižovat jeho výkonnost, což představuje jednu z hlavních nevýhod. Naopak ale nabízí větší možnosti v rozšiřování a výběru funkcí na daném počítači. Náklady na pořízení jsou menší než u hardwarové varianty, náklady na údržbu a administraci jsou částečně vyšší. (Přibyl ©2010)

Mimo výše popsaných druhů lze ještě firewall rozdělit do dalších kategorií dle využité technologie. Tyto technologie dělíme na:

- paketové filtry;
- aplikační brány;
- stavové paketové filtry.

Základ představuje **paketový filtr**, který je postaven na principu kontroly paketů procházejících přes firewall. Tuto kontrolu provádí dle bezpečnostních pravidel, která má nastavena správcem sítě, nebo počítače. Z hlavičky paketů si vezme IP adresu a port, na který soubor přichází, tu pak vyhodnotí a paket pustí dále, nebo ne. Dále může vyhodnocovat, od kterého zařízení v síti smí přijímat pakety, popřípadě na které místo nesmí pakety posílat. Jak uvádí zdroj, jde spíše o první hrubou selekci obsahu, který je puštěn do sítě, popřípadě k některému ze zařízení. Podrobnější filtrování zaručují **aplikační brány**, které umí navíc zahodit i pakety s obsahem nevyhovujícím danému nastavení, jak uvádí zdroj. (Peterka 2001)

5.3 Aktualizace

Ať už uživatel používá jakýkoliv druh software, je třeba, aby ho pravidelně aktualizoval, což u antiviru platí dvojnásob. Aktualizace antivirové databáze obsahují definice nově objevených virových infekcí, se kterými potom antivir porovnává nalezené infekce. U antiviru je dobré mít nastavené automatické aktualizace, u které program po připojení zkontroluje, zdali není nová verze virové databáze k dispozici a tu potom neprodleně stáhne. Pokud se jedná o aktualizace ostatního software v počítači, tak ty obsahují různé záplaty a opravy chyb, nebo v sobě nesou změněnou funkcionalitu programů. U záplat a oprav není nutné tolik rozvažovat, zda jsou potřebné, i když může docházet k případům, kdy aktualizace není povedená, nebo může způsobit nějakou jinou chybu. Při instalaci jiné funkcionality programu je nutno rozvážit, jak se ten dál bude chovat a zdali je nové chování žádoucí pro další práci s tímto programem.

Kontrolní otázky

Jaké jsou druhy antvirového software a co o nich víte?
K čemu slouží sandbox a karanténa?
Jaké má antivirový program možnosti práce s nakaženým souborem?
Jaký je hlavní rozdíl mezi heuristickou analýzou a testem integrity?
Co je to online testování a jaká nese úskalí?
Co je to firewall?

Souhrn

V této kapitole jste se dozvěděli, jak je důležité mít v počítači aktualizovaný software. Dále jste získali přehled o tom, jak funguje antivirová kontrola a některé další kontroly běžící na pozadí, jež se starají o bezpečnost vašich dat a informací.

Literatura a zajímavé odkazy

Problematika firewall - paketového filtru je popsána a zobrazena na následujícím videu Life of an IP packet v čase od 8:45 do 10:15 dostupného na WWW:<https://www.youtube.com/watch?v=9BGWrLiT9qs>. Na videu je také zobrazena cesta paketů po síti a způsoby, kterými se pakety dostávají na určené místo.

6 Webový prohlížeč a jeho bezpečnost

Cíle

Po prostudování této kapitoly:

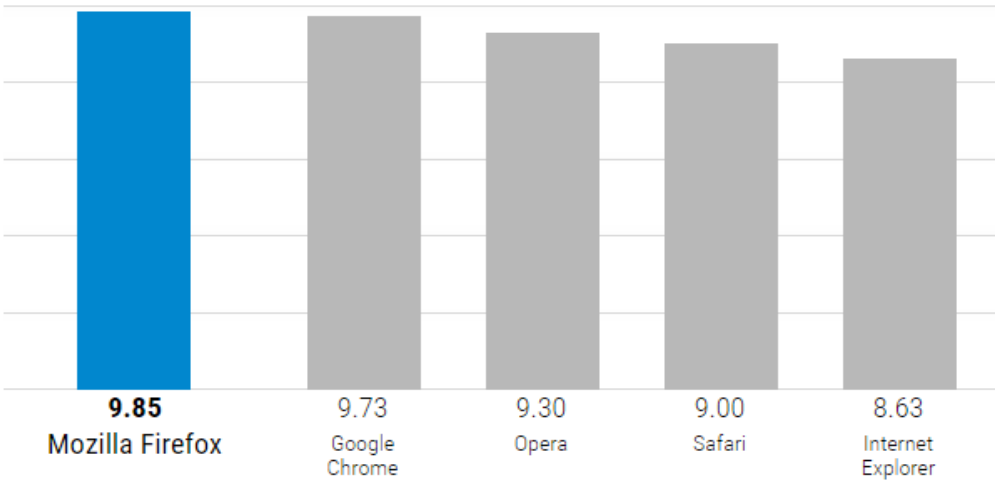
- Získáte přehled o vlastnostech vybraných webových prohlížečů.
- Zjistíte, k čemu tyto prohlížeče slouží.
- Dozvíte se, co jsou to cookies.

Pojmy k zapamatování

- Webový prohlížeč
- Cookies

6.1 Úvod k webovým prohlížečům

Webové stránky na internetu jsou naprogramovány pomocí různých značkovacích jazyků, popřípadě skriptů v kombinaci s programovacími jazyky. Aby si uživatelé mohli zobrazovat obsah těchto webových stránek (od textů přes obrázky, zvukový projev až po videa), čili ho neviděli jen jako změť znaků a byl pro ně čitelný, je nutné, aby měli v počítači, popřípadě jiném zařízení s připojením k internetu, nainstalovaný webový prohlížeč. Na následujících obrázcích je srovnání nejvyužívanějších webových prohlížečů.



Obrázek 9: Porovnání nejvyužívanějších prohlížečů

Zdroj: <http://internet-browser-review.toptenreviews.com/>, *upraveno*

Na obrázku jsou seřazené prohlížeče webových stránek podle celkového hodnocení, to zahrnuje tedy dále vyjmenované charakteristiky. Pořadí prohlížečů se shoduje i s hodnocením dle rychlosti a kompatibility a také podle bezpečnosti. Zdroj dále uvádí, že prohlížeče byly hodnoceny konkrétně z těchto hledisek (Carlsen 2015):

- rychlost načítání stránek a jejich obnovování, kombinovatelnost s hlavními zástupci z oblasti operačních systémů;
- další možnosti jako například správa záložek, rodičovská kontrola a RSS zdroje;
- bezpečnostní hlediska, tedy blokování vyskakovacích oken a škodlivého software;
- technická podpora a pomoc v podobě návodů a doplňkových textů.

Následuje přehled pěti prohlížečů z obrázku, který obsahuje souhrnné informace. Další informace lze nalézt na webech jednotlivých prohlížečů, popřípadě společností, které je vyvíjejí a které jsou uvedené u každého prohlížeče.

6.1.1 Mozilla Firefox

Obrázek 10 – Logo Mozilla Firefox
Zdroj: <http://internet-browser-review.toptenreviews.com/mozilla-firefox-review.html>

Firefox pochází od společnosti Mozilla Corporation.

Zdroj uvádí jako hlavní výhodu jednoduchost, rychlost a intuitivní ovládání. Prohlížeč nabízí možnosti využití velkého množství doplňků, které nepochází jen od společnosti Mozilla, jedním z nich je například Adblock Plus, který umí při správném nastavení zablokovat zobrazování reklam. Prohlížeč nabízí rychlé surfování po webových stránkách a při novém spuštění možnost zobrazení posledních navštívených jako skupiny stránek otevřených v jednotlivých kartách, které navíc umí seskupovat do skupin (známé jako Panorama). Prohlížeč umožňuje zobrazovat obsah PDF souborů. (Bloomfield 2015a)

Co se prohlížení webů týče, nabízí tyto možnosti: fulltextové vyhledávání dle hesel, možnost umístění komentářů a štítků k různým stránkám. Z bezpečnostních vlastností se jako největší výhoda jeví tyto: prohlížení webových stránek v anonymním režimu, po kterém nezůstávají v prohlížeči stopy, jako jsou uložená hesla, historie a cookies, o kterých bude dále ještě řeč, dále pak ochranu proti škodlivému software a bezpečnostní informace o webových stránkách ještě než je uživatel navštíví. Samozřejmostí je pak nastavení omezení při surfování pro děti, takzvaná rodičovská kontrola, kde lze omezit, co všechno smí potomci na internetu shlédnout. (Bloomfield 2015a)

Zajímavým doplňkem může být možnost využít na dotykových zařízeních takzvaná vícedotyková gesta, korekci pravopisných chyb a také hlasové povely. Při správném použití nám prohlížeč umožňuje i velké možnosti synchronizace různých nastavení. Samozřejmost představují automatické aktualizace a technická podpora. (Bloomfield 2015a)

6.1.2 Google Chrome

Obrázek 11: Logo Google Chrome

Zdroj: <http://internet-browser-review.toptenreviews.com/google-chrome-review.html>

Chrome pochází od společnosti Google.

Je rovněž velice rychlým prohlížečem, což není na úkor jednoduchého ovládání. Také má již integrovanou čtečku PDF souborů a navíc také přehrávač souborů typu Flash. Pokud si uživatel vytvoří účet na stránkách Google, může si zřídit vlastní profil a poté ho využívat při přechodu mezi zařízeními, nebo při půjčování počítače v jedné domácnosti. Odpadají tak dohady o tom, kdo provedl jaká nastavení a komu toto nastavení nevyhovuje. Vedle položky oblíbené a možností práce se záložkami nabízí navíc prohlížeč možnost tvořit si efektivní zástupce aplikací na ploše. (Bloomfield 2015b)

Co se týče práce se záložkami a více otevřenými kartami nabízí prohlížeč jednoduché otevírání v jiném okně, popřípadě přetahování mezi okny. Za zmínku také stojí to, že pokud uživatel otevře novou kartu pomocí odkazu na prohlížené stránce, tak ta se zařadí hned za tu prohlíženou. Je to obdoba seskupování ve Firefoxu. (Bloomfield 2015b)

Samozřejmostí je také anonymní režim bez zanechání stop po surfování v prohlížeči. Je třeba mít na paměti, že to ale neznamená, že nezůstávají stopy po surfování na serveru. Mimo bezpečnostních opatření proti škodlivému software nabízí tento prohlížeč také možnost otevírat webové stránky v sandboxu, jehož funkce byla popsána v kapitole o antivirovém software. Program se také automaticky aktualizuje a nabízí velké možnosti technické podpory, která je i pro začátečníky i pro zkušené uživatele. (Bloomfield 2015b)

6.1.3 Opera

Obrázek 12: Logo Opera

Zdroj: <http://internet-browser-review.toptenreviews.com/opera-review.html>

Opera pochází od společnosti Opera software.

Po Internet Exploreru je druhým nejstarším prohlížečem. Nabízí velké možnosti kompatibility napříč počítači i operačními systémy. Na rozdíl od dvou předešlých prohlížečů, není zpočátku tak intuitivní, což se ale zlepšuje s počtem času stráveným prací s tímto prohlížečem. Co se ovládání týče, nabízí také možnosti využívat jen klávesové zkratky, nebo hlas. Jako předchozí umí odfiltrovat škodlivé weby. Technická podpora není tak široká, ale má v nabídce prémiovou podporu. (Bloomfield 2015c)

6.1.4 Safari

Obrázek 13: Logo Safari

Zdroj: <http://internet-browser-review.toptenreviews.com/safari-review.html>

Safari pochází od společnosti Apple Inc.

I tento prohlížeč splňuje nároky na rychlost a intuitivnost ovládání. Nabízí možnost ukládat webové stránky pro pozdější čtení. Také umí upozornit na pravopisné chyby a uchovávat a spravovat uložená hesla. Slabou stránku představuje systém rodičovských kontrol a omezení surfování. Samozřejmostí je ale oproti tomu ochrana před škodlivým kódem. (Bloomfield 2015d)

6.1.5 Internet Explorer

Obrázek 14: Logo Internet Explorer

Zdroj: <http://internet-browser-review.toptenreviews.com/internet-explorer-review.html>

Internet Explorer pochází od společnosti Microsoft Corporation.

Nejdelším vývojem prošel tento prohlížeč, což se někdy projevovalo ustrnutím, protože pokud se někdy zabýváme dlouhou dobu jednou věcí, tak jí bývame unaveni. Je integrován v operačním systému Windows a stal se tedy hodně používaným, což vedlo k tomu, že se také stal cílem mnoha útoků škodlivého software, čemuž se snaží bránit díky bezpečnostním záplatám a aktualizacím. Jeho vývoj došel tak daleko, že detekuje phishingové útoky. Samozřejmostí je také rodičovská kontrola. Svou integrací do Windows splňuje využitelnost pro použití na dotykových obrazovkách, jelikož i Microsoft se částečně vydal cestou dotykového ovládání. (Bloomfield 2015e)

6.2 Cookies

Webové prohlížeče vedle hesel s historie procházení ukládají takzvané cookies. To jsou informace o navštívených stránkách a surfování mezi nimi. Jsou v nich data o uživatelských profilech a nastaveních. Ukládají se do počítače uživatele, popřípadě na serveru, se kterým komunikoval. Právě ukládání cookies může představovat jednu z cest, na kterou se zaměřují útočníci. Každý webový prohlížeč si totiž ukládá o návštěvách webů různé informace. O cookies více pojednává takzvaný RFC soubor. RFC jsou soubory popisující práci s weby, obsahují různá doporučení.

Kontrolní otázky

Co jsou to cookies?
K čemu slouží rodičovská kontrola?
Mají prohlížeče ochranu proti škodlivému software?
Jaké znáte webové prohlížeče, krátce je charakterizujte.

Souhrn

V této kapitole jste se dozvěděli, k čemu se využívá webový prohlížeč. Dále jste získali přehled o pěti vybraných prohlížečích. Doplnili jste také své znalosti o tom, co jsou to cookies a jaké znamenají bezpečnostní riziko při správném používání.

Literatura a zajímavé odkazy

O cookies konkrétně tedy pojednává RFC 2965 s názvem HTTP State Management Mechanism z října 2000 dostupný v anglickém jazyce na https://www.ietf.org/rfc/rfc2965.txt.

7 Bezpečnost nákupů přes internet a internetového bankovnictví

Cíle

Po prostudování této kapitoly:

- Dozvíte se jaké kroky podniknout při nakupování na internetu.
- Seznámíte se s klíčovými kritérii pro výběr spolehlivého prodejce.
- Dáte si pozor na bezpečnostní opatřeních při placení kartou přes internet.
- Budete informováni o zásadách bezpečného užívání internetového bankovnictví.

Pojmy k zapamatování

- zbožový srovnávač
- 3D Secure
- CVV/CVM kód
- Banker
- SSL

7.1 Nakupování online

Nakupování na internetu skýtá řadu výhod. Je rychlé, cenově výhodné, ušetří zákazníka zdlouhavých front v obchodech a nákupních centrech, nabídka výrobků je zde širší než v kamenných obchodech a vše je možné zařídit z pohodlí domova. Spolu s výhodami s sebou ovšem nese také četná rizika, kterým se však lze úspěšně bránit při dodržování zásad bezpečnosti.

7.1.1 Jak rozpoznat důvěryhodného prodejce?

Jednou ze zásad bezpečného nákupu, je využívání služeb prověřených internetových obchodů. Pokud nemá vlastní zkušenost s nákupem zákazník ani nikdo v jeho okolí, je vhodné vyhledat alespoň recenze obchodu a jeho hodnocení od ostatních uživatelů.

Dalším ukazatelem důvěryhodnosti jsou údaje, které o sobě prodejce zveřejní. Tyto informace by měly obsahovat název firmy, či jméno podnikatele, adresu a IČO firmy a telefonní číslo (Bezpečný internet [b.r.]). Uvedené údaje je vhodné prověřit (d TEST 2011, 40). Chybět by neměl také název a charakteristika nabízeného zboží, jeho cena včetně informací o dani a poplatcích a interval, ve kterém je uvedená cenová nabídka platná (Právní linka 2014).

Známkou spolehlivosti internetového obchodu je také certifikace. V České republice se na udílení certifikací zaměřuje Asociace pro elektronickou komerci - APEK, která na svých webových stránkách zveřejňuje seznam prodejců s touto certifikací. Seznam certifikovaných obchodů nalezneme také na stránce Certifikovaný obchod.cz Takto certifikované obchody bývají označeny logem certifikátu APEK (Apek ©2015).

Obrázek 15 – Logo certifikátu APEK
Zdroj: http://www.apek.cz/

Službu pro ověření spolehlivosti prodejců nabízí také Heuréka.cz která na základě hodnocení zákazníků uděluje certifikáty Ověřeno zákazníky. Další známkou, kterou Heuréka uděluje je Garance nákupu (Heureka blog 2013).

Obrázek 16 – Loga Ověřeno zákazníky a garance nákupu
Zdroj: http://blog.heureka.cz/category/sluzby-funkce/hodnoceni-obchodu-recenze/

Také v oblasti certifikace dochází k podvodům. Některé e-shopy mohou logo certifikátu zneužívat, proto je vhodné certifikaci prověřit, viz výše (Podnikatel.cz 2013).

Evropské spotřebitelské centrum na svých webových stránkách nabízí nástroj **Howard**, který má rovněž pomoci při vyhledávání informací o prodejci (cz.theshoppingassistant.com). Centrum také nabízí bezplatnou pomoc při problémech se zahraničními prodejci v rámci Evropské unie (Evropské spotřebitelské centrum [b. r.]).

7.1.2 Výběr zboží

Také zde není na škodu prostudovat recenze a uživatelská hodnocení výrobků, o něž má nakupující zájem. Vhodným ukazatelem, dle kterého se lze řídit je cena. Podezřelé by mělo být příliš drahé, ale také příliš levné zboží. Pro srovnání cen je možné využít zbožové srovnávače jako je Srovnání cen (www.srovnanicen.cz), Zboží.cz (www.zbozi.cz) Heuréka (www.heureka.cz) či Hledejceny.cz (www.hledejceny.cz).
Důležité je prostudovat bedlivě obchodní podmínky a reklamační řád. Je třeba sledovat, zda tyto podmínky splňují vše, na co má zákazník ze zákona nárok. Případné rozpory by měly vzbudit nedůvěru zákazníka.

7.1.3 Platba zboží

Možností je hned několik. V případě odběru zboží z neprověřeného obchodu bude lepší provést první platbu formou dobírky (Bezpečný internet [b. r.]).

Platba kartou je vhodná pouze u prověřených obchodníků. V případě že prodejce vyžaduje výhradně platbu předem, stojí za zvážení ustoupit od koupě (d TEST 2011, 41).

Platbu přes internet umožňují karty obsahující třímístný **CVV/CVC kód**, který je uveden na zadní straně karty. K platbě jsou zapotřebí ještě dva další údaje: šestnáctimístné číslo platební karty a datum, do kdy je karta platná. Všechny potřebné údaje jsou uvedeny přímo na kartě. V případě odcizení těchto dat má pachatel v rukou vše potřebné pro zneužití karty pro platbu přes internet. Při ztrátě je nutné kartu co nejdřív blokovat! K provedení platby však není nutné odcizit kartu. Stačí zaznamenat pro platbu potřebné údaje. Při platbě kartou je proto nejdůležitější ověřit, zda má internetový obchod, ve kterém nakupujeme, zabezpečený přenos dat při provádění plateb (Nováková 2011).

Obrázek 17 – Ukázka CVV/CVC kódu na zadní straně karty

Zdroj: <https://www.csas.cz/banka/nav/osobni-finance/visa-classic/jak-zaplatit-kartou-na-internetu-d00018657>

Možnosti ochrany jsou následující:

- **Protokol SSL (Secure Socket Layer)** s kterým jsme se setkali již v úvodní kapitole. Přenos informací o platební kartě je prostřednictvím certifikátu šifrován a nehrozí jeho zneužití. Zopakujme, že se pozná se podle malé značky zamčeného zámku nebo podle písmene http**s** na začátku adresy stránky. Uživatel se na stránkách e-shopů může setkat také se SSL certifikáty s ověřením společnosti. Jedná se o ověření SSL certifikátu důvěryhodným zdrojem, který se zobrazí ve webovém prohlížeči. Třetím typem je SSL certifikát s rozšířeným ověřením, který se pozná podle zeleného zbarvení příkazového řádku a garanta certifikátu, který rovněž uveden v příkazovém řádku (SSLS ©2006 – 2015).

Obrázek 18 – SSL certifikát s rozšířeným ověřením

Zdroj: https://www.ssls.cz/zeleny.html

- **3D-Secure** zabezpečení se pozná podle log karetních asociací Verified by Visa, Mastercard secure code. V tomto případě nezadáváte údaje o své kartě

obchodníkovi, ale přímo jeho bance, která bude příkaz zpracovávat. Údaje jsou navíc šifrovány. Pro uskutečnění platby je třeba zadat jednorázový SMS kód (Česká spořitelna [b. r.], Nováková 2011).

Obrázek 19 – Loga upozorňující na zabezpečení 3D Secure
Zdroj:http://www.ivasekartapomuze.cz/banka/appmanager/portal/jpk?_nfpb=true&_pageLabel=jpk_doc&docid=internet/cs/sc_13340.xml

Další možnost ochrany představuje nastavení denního limitu prostřednictvím internetového bankovnictví – maximální částka, kterou můžete utratit se rovná také maximální denní částce, která vám může být ukradena, pokud dojde ke zcizení údajů. Některé banky umožňují nastavit změnu limitu na konkrétní časový úsek, který si zvolí zákazník. Po uplynutí přednastaveného limitu se denní limit vrátí k původnímu nastavení (Bezpečný internet [b. r.]).

Variantou je rovněž převod příkazem prostřednictvím internetového bankovnictví. Obecné zásady jeho bezpečnosti uvedeme v další podkapitole.

K platbám a manipulaci s bankovními údaji je vhodné používat pouze soukromý počítač, to ovšem platí pro ochranu přístupových údajů obecně.

7.1.4 Doprava a převzetí zboží

Pro doručení je u nás možné využít zásilkových služeb DPD, PPL a České pošty. Mnoho internetových obchodů v současnosti umožňuje osobní odběr zboží na určených výdejních místech. U nás je tento způsob odběru velmi oblíbený a dlouhou dobu byl zcela bez poplatků. Přestože přibývá e-shopů, které, zpoplatnily osobní odběr, stále se jedná o nejméně nákladný způsob dopravy (Buřínská – Svoboda 2013; Právní linka 2014).

Při převzetí zásilky je doporučeno zboží ihned zkontrolovat. Ujistěte se, zda cena doručeného zboží odpovídá ceně objednávky. Ověřte také, zda zásilka není viditelně porušena. V takovém případě není vhodné zásilku přebírat. S dopravcem sepište protokol, o události zpravte také prodejce (APEK 2015). Ten zodpovídá za vzniklé vady až do okamžiku, kdy je zboží předáno zákazníkovi a je tedy zodpovědný za poškození zboží vzniklé během přepravy (dTest 2011, 41).

Zákazník má ze zákona nárok odstoupit od smlouvy a vrátit zboží do čtrnácti dnů od jeho převzetí a to bez udání důvodu (APEK 2015). V tomto případě máte rovněž nárok na vrácení poštovného a balného – ovšem pouze v nejnižší hodnotě nabízeného způsobu dopravy. Náklady vynaložené na vrácení zboží prodejci hradí zákazník. Odstoupení od smlouvy není možné v případě některých druhů zboží. Sem řadíme noviny, časopisy, výrobky upravené na míru klientovi, zboží, které s nízkým datem trvanlivosti, ale také audio a video nosiče, pokud byly vyjmuty z původního obalu (Právnická linka 2014).

7.2 Internetové bankovnictví

Internetové bankovnictví poskytuje časově neomezený přístup k většině poskytovaných bankovních služeb. Z toho důvodu jeho užívání na místě opatrnost.

Zabezpečení internetového bankovnictví se skládá z kombinace různých ochranných prvků. Zabezpečení účtů poskytovaných různými bankami se liší. Obecně se však jedná o přihlašovací údaje skládající s ID uživatele a hesla, či z bezpečnostního hesla a certifikátu. Přístup bývá rovněž chráněn prostřednictvím jednorázových kódu zasílaných prostřednictvím SMS. Možností je také přístup s pomocí čipové karty a čtečky. Rovněž změny v platebních transakcích bývají podmíněny zadáním kódu či vlastnictvím certifikátů (Bezpečný internet [b. r.]).

Přestože je přístup k internetovému bankovnictví chráněn poskytovatelem (např. SSL certifikát s rozšířenou validací), jsou zde další faktory, které díky kterým může uživatel utrpět značné škody. Poskytovatelé internetového bankovnictví nabízejí poradenství ohledně bezpečnosti užívání internetového bankovnictví. Jeho prostřednictvím také informují klienty o potenciálních hrozbách.

Nejčastější nebezpečí představuje odcizení přístupových údajů. K získání těchto údajů slouží prostředky označovaná jako **banker**. Útok může probíhat různě, nejčastěji prostřednictvím **keyloggerů** (Krčma 2012). Nebezpečný je také phishingový útok, viz výše.

Internetové bankovnictví může být ohroženo chybnou funkcí softwaru, přítomností virů, hrozbou je také lidský faktor.

Proto je nezbytné:

- Pravidelně aktualizovat antivirové programy, operační systém či prohlížeč a podobně. Neužívejte nelegální programy nebo programy z neověřených zdrojů. Pravidelně testujte zařízení na přítomnost virů.
- Mýt se na pozoru před physhingovými a podobně cílenými útoky (viz kapitola (viz kapitola 3.2.3). Kontrolujte, zda se přihlašujete skutečně prostřednictvím oficiální a chráněné stránky. Ty bývají v rámci útoků často padělány. Nikdy nedůvěřujte e-mailům, které vyžadují přístupové údaje k vašemu účtu. Banka takto nikdy nejedná. Podezřelé přílohy je lepší vůbec neotvírat.
- Chránit veškeré přístupové údaje! Nesdělujte je druhé osobě. Nebezpečný je rovněž přístup k internetovému bankovnictví prostřednictvím veřejného počítače či počítače připojeného na veřejnou síť. Chraňte elektronické certifikáty, pokud je využíváte k zabezpečení přístupu.
- Vytvářejte dostatečně silné heslo, jak bylo vysvětleno v úvodní kapitole. Heslo pravidelně obměňujte.
- Pravidelně sledujte pohyb financí na účtu. V případě nesrovnalostí nečekejte a účet co možná nejdříve zablokujte.
- Při zadávání příkazů buďte pozorní a zadanou transakci raději několikrát zkontrolujte. Navrácení peněz, které byly zaslány na jiný účet, než bylo zamýšleno, je zdlouhavé a komplikované (Air Bank 2013, Česká národní banka ©2003-2015).

Kontrolní otázky

Jaká jsou kritéria pro výběr spolehlivého obchodníka? Jak se zachovat při nespokojenosti s doručeným zbožím? Jak platit bezpečně platební kartou přes internet? Na co je třeba dát si pozor při práci s internetovým bankovnictvím?

Souhrn

Při nákupu přes internet je třeba věnovat čas pečlivému výběru obchodníka. Spolehlivého obchodníka indikují příznivé recenze a pravdivě uvedené informace o firmě. O vhodnosti nákupu svědčí také certifikace či zabezpečení platby kartou prostřednictvím SSL či 3D Secure. Při nákupu přes internet má zákazník ze zákona nárok na odstoupení od smlouvy do čtrnácti dnů od převzetí zásilky.

Nejzranitelnějším místem internetového bankovnictví je uživatel. Proto by měl dbát zásad bezpečnosti: chránit svůj počítač aktualizovanými antiviry, nepřipojovat se z nedůvěryhodných míst, nereagovat na podezřelé výzvy a nikomu nesdělovat přihlašovací údaje. Důležité je účet pravidelně sledovat a nežádoucí aktivity hned hlásit.

Literatura a zajímavé odkazy

Asociace pro elektronickou komerci APEK poskytuje poradenství a umožňuje ověřit pravost certifikátu internetových prodejců: www.apek.cz. Informace o online nákupech poskytuje na svém blogu také **Heuréka:** blog http://blog.heureka.cz/. Obecné rady pro spotřebitele a různá upozornění naleznete také na: spotrebitele.dtest.cz

8 Kyberprostor – funkce a rizika

Cíle

Po prostudování této kapitoly:

- Získáte povědomí o funkcích kyberprostoru a jeho schopnosti produkovat kulturu.
- Budete se orientovat v jeho základních psychologických rysech.
- Pochopíte, jak tyto rysy souvisejí s rizikovým chováním, kterého se někteří uživatele dopouštějí.
- Podrobněji se seznámíte s některými z rizik.

Pojmy k zapamatování

- Kyberprostor
- MMORPG
- Disinhibiční efekt
- Kyberkultury
- Digital divide
- sexting
- Netiketa
- Generace always on
- kybergrooming

8.1 Internet a kyberprostor

Za poměrně krátkou dobu se internet z pouhého experimentu proměnil na významnou součást každodenního života napříč kulturami. Co však způsobilo tuto expanzi? Nezbývá než uznat, že možnosti internetu jsou vskutku široké. Je nejen nástrojem komunikace (sociální sítě, virtuální světy), poskytuje také prostor pro práci, vzdělávání a trávení volného času (počítačové hry, MMORP) (Šmahaj 2014, 18). Jakožto kulturní prostředí umožňuje vznik různých skupin, komunit a subkultur a to v celosvětovém měřítku. Je vnímán jako součást procesu socializace (Jirovský 2007, 35; Šmahaj 2014, 13).

Internet je *„masové hypermédium, které vytváří kyberprostor a zároveň je jeho součástí“* (Šmahaj 2014, 16).

P. Greenfield a Z. Yan zase označují internet za kulturní nástroj, neboť sdílí a rozvíjí normy, které jsou následně přenášeny na další generace uživatelů. Noví uživatelé, nárůst jejich počtu a rozvoj technologií spoluvytvářejí nové normy, které jsou dále sdíleny a rozvíjeny (Greenfield – Yan 2006, 392).

V souvislosti s internetem a kyberprostorem hovoříme také o kyberkultuře. Ta představuje „soubor technik (materiálních i intelektuálních) praktických zvyklostí, postojů, způsobů uvažování a hodnot, které se rozvíjejí ve vzájemné vazbě s růstem kyberprostoru“ (Šmahaj 2014, 11).

Normy a pravidla chování v kyberprostoru tedy vytvářejí jeho uživateli (Jirovský 2007, 34). V souvislosti s tím hovoříme o tzv. netiketě. Netiketa přestavuje „neoficiální akceptovaná pravidla vhodného on-line chování“. Na jeho dodržování spolu s uživateli dohlížejí také poskytovatelé a správci služeb (Šmahaj 2014, 12). Vhodné uplatnění netikety může například pomoci snížit negativní disihibici, viz níže. J. Šmahaj dodává, že pravidla mohou být i zneužita agresory při snaze o vyloučení jedince z on-line skupiny, jak si ukážeme v kapitole věnující se šikaně (Šmahaj 2014, 21).

Způsob jakým v kyberprostoru vznikají a šíří se kulturní prvky má svá vlastní pravidla a přestože do jisté míry odráží offline svět, vše zde funguje jinak. Zajímavou definici kyberprostoru, která bere v potaz odlišnost od offline světa a jeho potenciální nebezpečí nabízí Václav Jirovský. Vnímá jej jako prostor, kam „se přenáší všechny rysy současné společnosti, ale život v kyberprostoru si formuje svoje vlastní pravidla, která se často vymykají přirozenému řádu, ve kterém lidské společenství žilo po staletí“ (Jirovský 2007, 16). Na jiném místě dodává „Otevřenost kyberprostoru potažmo internetu, spolu s jeho interaktivitou vede k domněnce, že kyberprostor je nejdemokratičtějším uskupením. Spíše by se však dalo hovořit o rozsáhlé anarchii v chování populace kyberprostoru, která nebýt omezována přísnými technologickými pravidly užívání, by kyberprostor již dávno zlikvidovala a učinila nepotřebným“ (Jirkovský 2007, 34).

8.1.1 Psychologické rysy kyberprostoru

Nyní se blíže podívejme na vlastnosti kyberprostoru, které ovlivňují prožívání dějů zde probíhajících. John Suler v této souvislosti hovoří o základních psychologických rysech kyberprostoru.

Jedním z nich je omezená percepce. Způsob, jakým probíhá komunikace v kyberprostoru, působí na naši schopnost vcítit se do druhé osoby. Limitovány jsou všechny smysly a to i v případě komunikace s využitím kamery a mikrofonu. Významnou a převažující součástí komunikace je písemný projev (Suler 1998). Omezená percepce může vést k chybnému vyhodnocení situace ale také k projekci našich vlastních představ a očekávání. Následkem uvedeného vnímáme naše online přátele jinak než by tomu bylo při osobní komunikaci (Šmahel 2003, 21).

S tím souvisí další rys, kterým je flexibilita identity. Kyberprostor nám dává příležitost kontrolovat mnohem více než v běžném životě, jakou část své identity odhalíme či zda si vytvoříme identitu jinou (Suler 1998).

Zajímavým stavem vyvolaným delší aktivitou na počítači je změněný stav vnímání, který může být podpořen a rozvinut možnostmi virtuálních světu a her (Suler 1998).

Zásadní vliv na chování uživatelů má také absence sociální stratifikace. Jediným kritériem hodnocení jsou zde komunikační schopnosti, intelektuální schopnosti a úroveň technického vybavení (Suler 1998).

Geografická vzdálenost uvnitř kyberprostoru nehraje roli. Také čas lze v kyberprostoru vnímat jinak než ve skutečnosti (Suler 1998). Hovoříme zde o synchronní a asynchronní komunikaci. Komunikace synchronní probíhá v téměř reálném čase prostřednictvím chatu a instant messengerů a podobně. Pro komunikaci asynchronní (e-maily) jsou typické větší časové prodlevy. V obou případech mají komunikující možnost se nad odpovědí zamyslet déle, než při rozhovoru tváří v tvář. Čas se tak může „natahovat“ ale také „smršťovat“ vzhledem k dynamické proměně kyberprostoru (Suler 1998, Hulanová 2012, 30).

Uživatel má možnost vést množství komunikací zároveň, aniž by si toho byli jednotliví účastníci konverzace vědomi. J. Suler tento jev nazývá sociální multiplicitou (Suler 1998). Zvláště nebezpečným nástrojem se z tohoto důvodu internet stává v rukou patologicky smýšlejících jedinců, jak si ukážeme v další kapitole.

Většina aktivit v kyberprostoru po sobě zanechává stopu. Lze rovněž vytvářet záznamy a ukládat je (Suler 1998). To s sebou nese pozitiva, ale rovněž může dojít k zneužití, viz níže.

V posledním bodě J. Suler poukazuje na možnost přerušení komunikace. Vždy hrozí, že se část komunikace ztratí či opozdí, což může u uživatelů vyvolat vlnu negativních reakcí (Suler 1998).

Některé z těchto rysů mají vliv na vznik takzvaného **disinhibičního efektu** (Suler 2004). Jedná se o opadnutí či snížení zábran, což umožňuje uvolněnější komunikaci o tématech, která mohou budit ostych či vyvolávají kontroverzi. Disinhibiční efekt se může působit pozitivně i negativně. Pozitivní vliv se projevuje ve zvýšené laskavosti, toleranci a porozumnění. Vyskytuje se častěji než negativní. K negativním důsledkům disinhibičního efektu řadíme například hrubé chování či vyhledávání stránek s násilným či pornografickým obsahem (Černá a kol. 2013, 33; Suler 2004).

S disinhibičním efektem se v běžném životě setkáváme také mimo internet. Zábrany opadají například ve skupině cizích lidí, o nichž víme, že je znovu nepotkáme.(Černá a kol. 2013, 16).

8.1.2 Soukromí a jeho odhalování na internetu

Charakter online prostředí dodává nový rozměr vnímání soukromí. Zatímco v běžném životě má soukromí jedince poměrně jasně vymezené hranice, ve světě internetu se ony meze jeví jako značně problematické (Ševčíková a kol 2014, 57). K informacím na internetu má totiž většinou přístup více stran (Ševčíková a kol. 2014, 58). Často skloňovaná anonymita internetu je tedy spíše osobním pocitem než reálnou hodnotou. Z toho důvodu je třeba rozlišovat anonymitu subjektivní (zahrnuje pocity a názory jedince) a anonymitu objektivní (reálný ukazatel možnosti identifikovat jedince s využitím dostupných technických nástrojů). Právě subjektivní anonymita souvisí s pocitem bezpečí, které mnoho uživatelů vnímá (Šmahel 2003, 19).

Proces odhalování soukromí na internetu se liší podle užitých médií. Medii, která k odhalování soukromí přispívají nejvíce, jsou sociální sítě (Ševčíková 2014, 58).

Sebeodhalování je přirozené a zvyšuje míru důvěryhodnosti a zmírňuje nejistotu. Vstřícnost v tomto ohledu vede v kyberprostoru ke zvyšování popularity. Nepřiměřené odhalování však může být vnímáno negativně. Vždy je třeba mít na paměti, že informace publikované na internetu se snadno šíří a mohou zde setrvat dlouhou dobu (Ševčíková 2014, 62).

8.2 Způsoby komunikace a prezentace v kyberprostoru

Internetová komunikace a probíhá prostřednictvím různých kanálů, které nabízejí rozličné funkce. Mezi ty nejčastěji užívané patří email, diskusní fóra a instant messengery - programy umožňující písemně komunikovat v reálném čase, patří sem ICQ, MSN, tuto funkci nabízí rovněž Skype. Instant messenger bývá součástí sociálních sítí (facebook); nabízí ho také například g-mail. Komunikace probíhá také v chatových místnostech a prostřednictvím různých diskusních fór, která v sobě spojují také možnost setkávání se s dalšími uživateli. Specifickým prostředím integrujícím v sobě množství funkcí poskytují sociální sítě.

8.2.1 Sociální sítě

Sociální sítě představují on-line prostor skýtající četné výhody virtuálního světa. Prostor, který je určen k setkávání a komunikaci lidí. Umožňuje sdílet zážitky a názory, fotografie či videa (Bezpečný internet [b.r.]). Mnoho uživatelů díky nim například navazuje nová přátelství či udržuje kontakty na velké vzdálenosti.

Vývojáři pružně reagují na potřeby svých uživatelů. V současné době je k dispozici skutečně pestrá škála sociálních sítí, z nichž si může každý vybrat podle svých zájmů a potřeb. Mezi nadnárodní sociální sítě nejčastěji užívané v České republice patří Facebook, Twitter, Google+, Instagram, Youtube, Badoo, LinkedIn, Pinterest a MySpace. Všechny uvedené sociální sítě s výjimkou MySpace nabízejí uživatelům svou českou mutaci či uživatelské rozhraní v češtině. Z původně českých sociálních sítí sem lze zahrnout Spolužáci.cz, Lidé.cz či líbímseti.cz.

Podle výzkumu MML TGI agentury Median, s. r. o. z roku 2014 patří mezi nejvíce užívané zahraniční sociální sítě v České republice Facebook a videoserver YouTube. Sociální sítí hojně užívanou mladou generací je twitter. 37% jeho uživatelů náleží do věkové skupiny 12 – 19 let. (Media Guru 2015).

Sociální sítě jsou běžným a hojně využívaným prostředkem k sebeprezentaci jedince i skupin včetně oficiální prezentace různých organizací. Právě z toho důvodu obsahují velké množství osobních informací, které mohou představovat potenciální riziko. Je proto důležité ověřit, jaké technické prostředky nám k ochraně soukromí mohou sociální sítě poskytnout. Uživatel sám by měl rovněž dodržovat zásady bezpečného chování. Tato pravidla lze s mírnými obměnami aplikovat také pro další formy internetové komunikace.

- Užívat dostatečně silná hesla, jak bylo doporučeno v úvodní kapitole.
- U sociálních sítí je obvyklé, že přístup k některým našim údajům mají také lidé, kteří nepatří k našim „přátelům“. Proto je třeba ověřit si nastavení soukromí v rámci sociální sítě a zjistit, kdo všechno může publikované příspěvky vidět (Skyba c1995 – 2015). Nastavení zabezpečení u čtyř oblíbených sociálních sítí se věnuje série drobných článků dostupných na stránkách časopisu PC World (Čepička 2013).
- Uveřejňovat informace a materiály týkající se osobního života s rozvahou. Profily na sociálních sítích mohou kromě přátel, přátel přátel zajímat také personalisty (Skyba c1995 – 2015; KarieraWeb.cz 2011).
- Nepublikovat informace, které byste nikdy nesdělili cizímu člověku.
- Nepřispívat na sociální síť pod vlivem omamných látek.
- Přihlašovat se pouze z důvěryhodných zařízení.

- Nesvěřovat hesla druhé osobě a nereagovat na výzvy pro potvrzení hesla (Szabó 2011).
- Při komunikaci s přáteli z online světa je třeba být obezřetný a ověřit si jejich totožnost.

Poslední bod může být problematický pro děti a mladistvé, kteří touží po popularitě mezi vrstevníky a v tomto ohledu mohou pociťovat také jistý sociální tlak. Mít na sociálních sítích hodně přátel, odběratelů či následovníků je pro ně otázkou společenské prestiže. V důsledku toho mohou ztratit obezřetnost a uzavřít virtuální přátelství s neznámou osobou, které tím otevře přístup k svým osobním údajům. Potenciální útočník tak získá možnost svou oběť anonymně sledovat (Rogers 2011, 34).

Velkou oblibu sociálních sítí u mladé generace ukazuje řada výzkumů. Většina dětí a mladistvých pro své potřeby využívá alespoň jednu sociální síť (Černá a kol. 2013, 28). Data získaná při výzkumu EU Kids Online II ukazují, že v České republice má svůj profil na sociálních sítích 72% dětí ve věku 9 -16 let (Ševčíková a kol. 2014, 23).

Šetření pracovníků pedagogické fakulty Univerzity Palackého v Olomouci vyplynulo, že 81% dotázaných dětí (kolik a jaké věkové rozmezí) užívalo v roce 2011 facebookový profil, 38,93% užívalo badoo. K užívání Myspace se hlásilo 14,46% dotázaných, a Líbím se ti.cz navštěvovalo dle svého tvrzení 12, 79%. (Szotkowski – Kopecký – Krejčí 2012, 38).

Vzhledem ke své funkci jsou sociální sítě pro mnoho uživatelů svázány s offline světem více než jiné internetové komunikační prostředky. Uživatelé zde vystupují pod vlastními jmény a komunikují zde se svými přáteli a známými. Sociální sítě tak do jisté míry reflektují vztahy v offline světě. Nejvíce to platí pro mladistvé, kteří je vnímají jako běžný nástroj každodenní komunikace. Sociální sítě tak „představují organickou součást sociálního života a také vývoje adolescentů“ (Ševčíková 2014, 59).

Poznámka

Nadměrné užívání informačních komunikačních technologií a sociálních medií může souviset s rozvojem některých psychických poruch, kam patří například obsesivní jednání, narcismus, poruchy pozornosti a hyperaktivita, zmožení mentálních identit (Trampota 2013). Hrozí také vznik závislosti, viz níže.

8.2.2 MMORPG a virtuální světy

Specifické prostředí zábavy umožňující sdružování a komunikaci představují MMORPG hry (Massively Miltiplayer Online Role-Playing Games) a virtuální světy. Tyto hry sdružují velké množství hráčů, kteří vzájemně komunikují, aby vytvářeli strategie a dosahovali společných cílů. V obou případech si hráč vytváří virtuální indentitu, kterou symbolizuje avatar – tedy postava, prostřednictvím které hráč působí ve virtuálním světě hry.

Mezi nejznámější zástupce MMORPG patří World of Warcraft či Everquest. Jako příklad virtuálního světa, jehož účelem je navazování kontaktů a komunikace uveďme Second life (Ševčíková a kol. 2014, 26).

Tyto hry patří k oblíbeným internetovým aktivitám mládeže. Anna Ševčíková uvádí, že takto tráví čas 69% dotázaných chlapců a 49% dívek. Virtuálním světům se věnuje 49% chlapců, ale pouze 9% dívek (Ševčíková a kol. 2014, 26).

Kyberprostor nabízí řadu lákadel, kterým mladý člověk jen těžko odolává. V. Jirovský vysvětluje atraktivitu kyberprostoru následujícím způsobem: *„Symbolický prožitek sice nemůže nabídnout plný prožitek skutečnosti, ale také minimalizuje případná rizika. V kyberprostoru se nemůže fyzickému jedinci nic stát, a tak může např. vystupovat na různých diskusních nebo chatových serverech v různých rolích, měnit svůj věk i pohlaví, a uskutečňovat vlastní představu o sobě.“* (Jirkovský 2007, 35). Ona minimalizace rizik, o níž autor hovoří, zřejmě spočívá v možnosti beztrestně experimentovat s vlastní identitou (Second life, hry) v rozsahu v jakém by nebyla v offline světě možná a také s pocitem subjektivního bezpečí, člověka sedícího za monitorem v pohodlí domova. Bohužel online svět se s offline světem prolíná mnohem více, než si připouštíme. Jak si ukážeme v následujícím textu, rizika spojená s užíváním internetu/kyberprostoru s sebou mohou nést závažné následky jak fyzické, tak psychické.

8.3 Rizika spojená s životem v kyberprostoru

Nejzranitelnější jsou děti a mladiství. Lidé, kteří se narodili po roce 1994, jsou označováni jako **generace always on**, nebo také **digital natives** (Šmahaj 2014, 13). Internet se pro mladou generaci stal integrální součástí jejich každodennosti. Děje v online a offline světě vnímají jako navzájem propojené a vyznačit mezi nimi přesnou hranici by mohlo být obtížné (Ševčíková a kol. 2013, 31).

Nebezpečí spočívá také v neporozumění starších generací. Prudký rozvoj digitálních technologií vyvolal jev označovaný jako **digital divide**. Vznikl mezigenerační rozdíl ve schopnosti porozumět a využívat rychle se vyvíjející informační a komunikační technologie. Jelikož ke zmíněnému jevu došlo velmi rychle, žijí vedle sebe dvě generace se zcela odlišným přístupem a návyky spojenými s užíváním těchto technologií (Šmahaj 2014, 13).

K tomu se váže jeden z mýtů o dětech a jejich aktivitách na internetu. Přestože je pravdou, že děti často rozumí internetu lépe než jejich rodiče, neznamená to, že vědí všechno. Poučení o bezpečném chování na internetu by se mělo stát součástí jejich výchovy (Livingston – Hadon 2011).

8.3.1 Sexting

Sexting představuje rizikové chování, které zahrnuje šíření textu, vlastních fotografií či videí se sexuální tematikou prostřednictvím internetu a mobilních telefonů (Szotkowski – Kopecký – Krejčí 2013, 81). První známé případy sextingu datujeme k roku 2005 (Hulanová 2014, 62).

Autor jejich zveřejněním a dalším šířením riskuje zneužití poskytnutých materiálů, které mohou posléze vést například k vydírání či kyberšikaně dotyčného (Szotkowski – Kopecký – Krejčí 2013, 81). Sexting může být zneužit také k šíření dětské pornografie. Podobné případům došlo také v České republice (Hulanová 2012, 62).

Výzkum pracovníků Pedagogické fakulty Univerzity Palackého v Olomouci odhalil, že v roce 2011 na internet umístilo materiály se sexuálním obsahem 8,25% dětí. Konkrétním osobám zmíněné materiály rozeslalo 9, 7% dětí. 73% procent dotázaných vnímalo toto chování jako rizikové (Szotkowski – Kopecký – Krejčí 2012, 24).

Sexting častěji provozují osoby starší patnácti let. Jako důvod této aktivity raspondenti uváděli nudu, snahu o navázání intimního kontaktu s druhou osobou, zmiňována byla také sebeprezentace (Szotkowski – Kopecký – Krejčí 2012, 24).

8.3.2 Závislost na internetu

O nadměrném užívání internetu hovoříme, pokud se v důsledku toho u uživatele dostaví „*fyzické, psychické či sociální problémy*“ Průměrná délka užívání internetu se u dětí a mladistvých pohybuje mezi jednou až dvěma hodinami denně (Ševčíková a kol. 2014, 38).

K nadužívání internetu jsou náchylnější jedinci s nízkým sebehodnocením, poruchami pozornosti a se zvýšeným sklonem nudit se. Jako řešení problému k němu tíhnou děti a mladiství se sklonem k sociální úzkosti, depresím či s problémy zapadnout do kolektivu (Ševčíková a kol. 2014, 39). Internet vyvolává falešný pocit anonymity a bezpečí, ke kterému se děti s uvedenými problémy mohou začít uchylovat. Nadměrné užívání internetu nicméně nepřispívá ke skutečnému řešení problému a z dlouhodobého hlediska vede spíše ke zhoršení situace (Ševčíková a kol. 2014, 40).

Ačkoliv nadměrné užívání internetu nemá na rozdíl od závislosti vliv na školní prospěch, je zde mnoho negativních důsledků. Nadužívání internetu negativně ovlivňuje spánkové návyky i kvalitu spánku v důsledku předchozích na soustředění náročných aktivit. Hrozí rovněž problémy s pohybovým aparátem (Ševčíková a kol. 2014, 42). Nadměrné užívání se může vymknout kontrole a přerůst v závislost (Ševčíková a kol. 2014, 44).

Lukas Blinka definuje závislost na internetu jako *„činnost, která se stane dominantní v životě dítěte, která je doprovázena změnami nálad a pro niž musí mladý uživatel internetu obětovávat stále více času, aktivit nebo vztahů.“* Neschopnost zmíněnou činnost vykonávat má za následek abstinenční příznaky. Typické je se k činnosti navracet i po období „abstinence“ (Ševčíková a kol. 2014, 44).

Velký problém představují MMORPG a jiné virtuální světy, které vyžadují poměrně velkou časovou dotaci.

Důležitá je prevence. Varování před nebezpečím závislosti by měla být zahrnuta do programů v rámci školní výuky. Důležité je také informovanost mezi rodiči, kteří mohou problému předejít, nebo ho alespoň včas odhalit (viz. rodičovská mediace v následující kapitole).

8.3.3 Kybergrooming

Kybergrooming je považován za jeden z nejnebezpečnějších jevů, s kterými se lze setkat na internetu a v prostředí moderních komunikačních technologií. **Kybergroomeři** či **predátoři** vystupující pod falešnou identitou zde hledají své oběti. Jejich záměrem bývá vyvolat v oběti pocit důvěry a vylákat ji na společnou schůzku. Pokud se jim to podaří, následky bývají fatální. Oběť může být fyzicky napadena, mučena, znásilněna, donucena k prostituci. V zahraničním kontextu jsou známy případy, kdy oběť nabádána k terorismu. Kybergrooming může skončit smrtí oběti (Szotkowski – Kopecký – Krejčí 2013, 50).

Kybergroomeři využívají různých služeb – vedle sociálních sítí to jsou například chatové místnost, internetové seznamky, herních portály či inzerční plochy.

Komunikace mezi predátorem a obětí probíhá různě dlouho – několik měsíců, ale i roky. Právě v trpělivosti kybergroomerů tkví velké nebezpečí. Za dlouhou dobu komunikace vnímá nic netušící oběť vztah jako důvěrný a přátelský, necítí tedy potřebu mít se na pozoru. Oběť postupně svěřuje kybergroomerovi svá tajemství. Pokud se útočníkovi manipulace s obětí nedaří, může přistoupit také k vydírání (Szotkowski – Kopecký – Krejčí 2013, 51 - 52).

Rozpoznat predátora je velice těžké, protože jediným společným znakem bývá patologický zájem o osoby mladší 18 let. Osob s pedofilními sklony se mezi kybergroomery pohybuje asi jen 10%. Mezi početnější skupinu spadají hebofilové či efebofilové. Ti se zaměřují na dospívající chlapce a dívky s plně vyvinutými druhotnými pohlavními znaky. Mezi kybergroomery najdeme osoby různého věku, pohlaví, vzdělání a společenského statutu. Mnozí z nich navíc nebyli nikdy trestáni (Szotkowski – Kopecký – Krejčí 2013, 52; Hulanová 2012, 57).

Útočník může vystupovat pod jednou identitou (**identita statická**), může však užívat různé identit (**identita dynamická**), které mění podle potřeby. Výrazné rozpory v online komunikaci proto není radno podceňovat. Predátoři mohou rovněž vystupovat jako zástupci firem či agentur (Szotkowski – Kopecký – Krejčí 2013, 56 – 57).

Kybergrooming spočívá v manipulativním jednání (Hulanová 2012, 52). Často užívanou technikou k navázání kontaktu a získání důvěry je **zrcadlení** leckdy označované anglickým termínem **mirroring.** Cílem je navodit pocit důvěry a zájmu. Predátor předstírá, že s obětí sdílí totožné zájmy, radosti i trápení. Často se v aktivitách dětí a mladistvých skutečně orientuje a díky přípravě je schopen komunikovat jejich jazykem. V získávání informací bývá velmi pečlivý. O svých obětech si může vést systematický přehled, sdělené informace dále doplňovat a ověřovat. Telefonní číslo či adresu si kybergroomeři ověřují například zasláním kreditu či dárku. Tato praktika se označuje termínem **luring** a kromě ověření kontaktu má rovněž zvýšit predátorovu důvěryhodnost a oblibu, či posloužit jako úplatek za poskytnutí dalších osobních informací (Szotkowski – Kopecký – Krejčí 2013, 60 - 61). Kybergroomer se také snaží izolovat svou oběť od okolí. Nabádání k udržení tajemství, tvrzení, že „je jediný, kdo to pochopí“ či přání uchovat konverzaci v tajnosti by mělo vzbudit ostražitost (Hulanová 2012, 53). Se vzrůstající důvěrou postupně přistupuje k intimnějším tématů. Postupně směřuje ke konverzaci sexuálního obsahu, svým obětem může rovněž zasílat pornografické materiály (Hulanová 2012, 53).

Jakmile útočník získá o své oběti dostatek informací, pokusí se přimět ji k schůzce. V tuto fázi musí překonat rozdíl jeho skutečného věku a věku, který udává v rámci své falešné identity. Jeho snahou tedy je přesvědčit oběť, aby důvěřovala jeho bratrovi, otci nebo třeba strýčkovi. K útoku nemusí dojít na první schůzce, predátor se naopak může nejprve snažit vztah ještě více posílit (Szotkowski – Kopecký – Krejčí 2013, 64).

Oběťmi se stávají stejnou měrou chlapci i dívky. Jejich věk se nejčastěji pohybuje mezi 11 – 17 lety. Tyto oběti mohou spojovat emocionální problémy, nízká sebedůvěra, přehnaná důvěřivost či ochota rozvíjet konverzaci na téma sexualita (Szotkowski – Kopecký – Krejčí 2013, 55).

Svěřování důvěrných informací neznámé osobě se v průzkumu EU Kids online ukázalo jako nejčastější rizikové chování u dětí (Livingstone – Haddon 2009, 3).

Je třeba vyvarovat se následujících aktivit:

- Sdělování osobních a intimních informací jedincům, které neznáme osobně;
- Publikování či rozesílání zpráv, fotografií či videí se sexuálním obsahem;
- Uskutečnění osobní schůzky se „známým z internetu“, pokud se dotyčný přeci jen rozhodne schůzku uskutečnit, měl by se dostavit s doprovodem
- Poskytování materiálu se sexuálním obsahem za úplatu (Hulanová 2014, 98).
- Odhalování intimních partií před webkamerou, byť by tak měl být učiněno na oplátku! (Szotkowski – Kopecký – Krejčí 2013, 62).
- Zajímavý pokus představuje vyhledání informací o vlastní osobě přes internetové vyhledavače. Pokus ukazuje, jaké informace se může dozvědět potenciální útočník.

Poznámka

Webcam trolling – počítačový program simulující webkameru, který vyvolává iluzi, že sledujeme přenos z webkamery, který probíhá v reálném čase. S využitím tohoto programu je možné pouštět různá videa. Kybergroomeři obvykle zneužívají skutečná videa mladistvých pořízená původně například za účelem sextingu. Cílem je přesvědčit oběť, že komunikuje s vrstevníkem, získat z oběti intimní fotografii či obnažení před webkamerou. Je pravděpodobné, že si predátor pořídí záznam celé akce. Záznamem poté může svou oběť vydírat. Nápadným znakem těchto podvodných rozhovorů přes webkameru je chybějící zvuk. Komunikace probíhá pouze písemnou formou (Szotkowski – Kopecký – Krejčí 2013, 62).

Dalším číhajícím nebezpečím je kyberšikana, které budeme vzhledem ke komplexnosti problému věnovat samostatnou kapitolu.

Kontrolní otázky

Vyjmenujte charakteristiky kyberprostoru.
Čím kyberprostor ovlivňuje naše vnímání?
V jakých konkrétních případech se setkáváme s disinhibicí?
Zamyslete se nad příklady z online i offline prostředí.
Jaká nebezpečí hrozí na internetu?
Jaká rizika představuje kybergrooming?
V čem spočívá jeho nebezpečí?

Souhrn

Kyberprostor představuje specifické prostředí, které svými charakteristikami do jisté míry ovlivňuje naše chování v tomto prostoru. Disinhibiční efekt má vliv na zmírňování zábran, což může vést k přílišnému sebeodhalování a s ním spojenému rizikovému chování jako je sexting. Toto chování může uživatele ohrožovat. Kromě závislosti hrozí také setkání s patologicky smýšlejícími jedinci. K velmi nebezpečným jevům, s nimiž se můžeme v kyberprostoru setkat, je kybergrooming.

Literatura a zajímavé odkazy

HULANOVÁ, L. *Internetová kriminalita páchaná na dětech. Psychologie internetové oběti, pachatele a kriminality.* Praha – Kroměříž: Triton, 2012. 217 s. ISBN 978-80-

7387-545-9
ŠEVČÍKOVÁ, Anna a kol.: Děti a dospívající online. Vybraná rizika používání internetu. Praha - Brno: Grada Publishing – Masarykova univerzita, 2014. ISBN 978-80-247-5010-1.

9 Kyberšikana

Cíle

Po prostudování této kapitoly:

- Získáte představu o podstatě kyberšikany.
- Budete si vědomi, jaké jsou rozdíly mezi šikanou a kyberšikanou.
- Budete obeznámeni s formami útoků a s prostředky pomocí kterých k útokům dochází.
- Dozvíte se jak v případě kyberšikany postupovat, jak se bránit a jaká přijímat preventivní opatření.

Pojmy k zapamatování

- Kyberškádlení
- Flaming
- Kyberharašení
- Kyberhádka
- Flame War
- Outing
- Online obtěžování
- Happy Slapping
- Rodičovská mediace

9.1 Co je to kyberšikana

Termín kyberšikana poprvé použil v roce 2001 kanadský pedagog Bill Belsey. Do stejného období přibližně spadají také počátky bádání v této oblasti. Oproti studiu šikany, které intenzivně probíhá již od sedmdesátých let minulého století, se jedná o poměrně mladou disciplínu. Z toho důvodu není zcela sjednocena metodika výzkumu ani pojmosloví (Černá a kol. 2013, 9-10). Spíše než zcela nová fenomén se kyberšikana jeví jako adaptace tradiční šikany na nové prostředí (Černá a kol. 2013, Šmahaj 2014, 65).

Poznámka

Kyberšikana se v žebříčku rizik online prostředí umístila jako čtvrtá (Livingstone – Heddon 2009, 3).

Abychom mohli kyberšikanu lépe pochopit, podívejme se nejprve na šikanu obecně. Průkopník výzkumu šikany Dan Olweus ve své práci vymezil tři základní znaky:

- Úmyslné jednání;
- dochází k němu opakovaně;
- nerovnováha sil mezi obětí a agresorem – oběť se nemůže bránit, protože agresor je silnější, starší, má významné postavení ve skupině a podobně (Černá a kol. 2013, 10; Olweus 1994, 9-10).

U kyberšikany se k znakům, které stanovil D. Olweus přidává skutečnost, že se tak děje prostřednictvím informačních a komunikačních technologií.

Dle B. Belseyho *„kyberšikana zahrnuje užití informačních a komunikačních technologií k záměrnému, opakovanému a nepřátelskému chování, vykonávanému jedincem nebo skupinou za účelem poškodit druhé“* (Belsey, [b.r.]).

Podobnou definici nabízí Megan Price a John Dalgleish: *„Kyberšikana je kolektivní označení forem šikany prostřednictvím elektronických médií, jako je internet a mobilní telefony, které slouží k agresivnímu a záměrnému poškození uživatele těchto médií. Stejně jako tradiční šikana zahrnuje i kyberšikana opakované chování a nepoměr sil mezi agresorem a obětí.“* (Price – Dalgleish 2010, 51 dle Černá a kol. 2013, 20).

K těmto kritériím někteří badatelé připojují další podmínku: oběť vnímá toto chování jako příkoří (Černá a kol. 2013, 21).

Ne každé agresivně působící chování, se kterým se na internetu setkáme, splňuje uvedené znaky kyberšikany. Jak jsme již zmínili, internet představuje zvláštní prostor s vlastními pravidly a tolerance agresivního chování je zde vyšší než v běžném životě (Černá a kol. 2013, 24; Šmahel 2003, 80).

9.1.1 Kyberškádlení

Kyberškádlení je obdobou popichování a škádlení v offline prostředí. Jeho cílem není ublížit a nedochází zde ani k mocenské nerovnováze. Může představovat součást zdravého vztahu mezi jedinci a pozitivně působí na rozvoj sociálních a komunikačních dovedností (Šmahaj 2014, 46, Černá a kol 2013, 24). V okamžiku, kdy toto škádlení přestává být příjemné a opakovaně se stává zraňujícím, lze jej klasifikovat jako šikanu. Problémem kyberprostoru je, že autor „žertu“ nevidí přímou reakci osoby, na kterou zacílil, dlouhodobě si tak ani nemusí být vědom, že se šikany dopouští (Černá a kol. 2013, 24).

9.1.2 Kyberhádka

Záměrem kyberhádky může i nemusí být touha zranit oběť. Kyberhádka probíhá jednorázově. Může však také přerůst ve flamming, který je klasifikován jako druh kyberšikany viz níže. (Šmahaj 2014, 46).

9.1.3 Online obtěžování x kyberobtěžování

Alena Černá užívá pojem **online obtěžování** v souvislosti s chováním, které splňuje všechna kritéria kyberšikany až na skutečnost, že jej oběť nevnímá jako zraňující (Černá a kol. 2013, 21). Pro obdobné chování, které však oběti ubližuje, užívají označení **kyberharašení** dle anglického cyberharrassment (Černá 2013, 26). Např. Jan Šmahaj pro stejný jev užívá označení kyberobtěžování (Šmahaj 2014, 46 – 47).

Z uvedených příkladů vyplívá, že hranice určující, jaké chování je již možné považovat za šikanu může být leckdy velmi tenká. Je třeba mít na paměti, že z důvodů snížené percepce v prostředí internetu si reakce druhé osoby pouze domýšlíme. Proto je třeba být v komunikaci velmi obezřetný.

Poznámka

Vzhledem k tomu, že je kyberšikana zkoumána poměrně krátce, nepanuje dosud mezi badateli shoda v přístupu. Definice kyberšikany a otázky, které si badatelé kladou

(spolu s časovým rozmezím sledovaného jevu či věkovými skupinami dotázaných) je obzvláště důležitá při srovnávání výsledků jednotlivých výzkumů. Rozdílně nastavené parametry přirozeně vedou k různým výsledkům, které pak nelze komparovat.

9.2 Specifika kyberšikany

Kyberšikana představuje komplexní jev, který může zahrnovat kombinaci přímé, nepřímé, verbální, pasivní i aktivní agrese (Chromý 2010, 41). Od šikany, tak jak je tradičně vnímána, se kyberšikana odlišuje hned v několika ohledech. Specifika jsou dána vlastnostmi internetu/kyberprostoru, ve kterém ke kyberšikaně dochází, ale také chováním uživatelů.

Mění se například charakteristika oběti. Zatímco šikana častěji zasahuje jedince odlišující se od většiny (například fyzicky slabé, neoblíbené v kolektivu a podobně). Oběti kyberšikany většinou spojuje pouze velké množství času stráveného na internetu a rizikové chování jako je zveřejňování osobních údajů a citlivých informací (Ševčíková 2014, 131). Obětí kyberšikany se ale může stát kdokoliv (Šmahaj 2014, 43; Chromý 2010, 41).

Jako jedno ze specifik kyberšikany je často uváděna anonymita agresora, což nemusí vždy platit. Například pokud kyberšikana navazuje na tradiční formu šikany, zná oběť identitu agresora velmi často. Případy, kdy je agresor neznámý se vyskytují méně často (Černá a kol. 2013, 49). Pokud však k takové situaci dojde, anonymita útočníka může oběť naplňovat nejistotou. Hrozí, že oběť postupně začne tuto nejistotu přenášet také do svého běžného života (Rogers 2011, 32). Možná anonymita (viz subjektivní anonymita v předchozí kapitole) také poskytuje útočníkovi pocit bezpečí. Navíc si není vědom, přímých dopadů na oběť, což minimalizuje jeho pocit viny. Také přihlížející nemusí včas odhalit závažnost skutku (Černá a kol. 2013, 24, 59-60).

Prostředí internetu také umožňuje, aby se role agresora ujala osoba, která toho není v běžném životě schopna například z důvodů nízké fyzické zdatnosti či špatného postavení v kolektivu, který by její agresivní chování nepodpořil (Černá a kol 2013, 92).

Dalším tíživým znakem kyberšikany je skutečnost, že oběť může být útokům vystavena téměř nepřetržitě. Agrese tak proniká i do prostředí, které bylo vnímáno jako bezpečné. Oběť se může následně potýkat s pocitem neschopnosti nalézt útočiště, což mnohdy vyústí v přesvědčení, že nikde a s nikým není bezpečno (Rogers 2011, 32). V tomto ohledu je nejvíce ohrožena mladá generace, která je připojena nepřetržitě, jak už jsme zmínili v předchozí kapitole (Černá a kol. 2013, 21). Odpojení od internetu se nejeví jako vhodné řešení. Kyberšikana jedince probíhá nadále i bez jeho přítomnosti. Odstranění urážlivého a ponižujícího materiálu je následně velmi problematické a někdy dokonce nemožné (Šmahaj 2014, 65 - 66). Možná anonymita a neomezený přístup k oběti naplňují kritérium mocenské nerovnováhy, jak jej vymezil Olweus viz výše (Černá a kol. 2013, 21).

Také kritérium opakování funguje v on-line světě odlišně. K jeho naplnění je poměrně snadné, protože nastane v okamžiku, kdy byl agresivní příspěvek umístěn a ponechán na veřejně přístupné stránce (blogu, sociální síti a podobně), kde ho mohou ostatní uživatelé vidět a dále na něj reagovat. Každá reakce schvalující a rozvíjející urážlivý obsah může oběť znovu zraňovat (Černá a kol. 2013, 21).

Tím se dostáváme k dalšímu problému. Zatímco oběť šikany bývá ponížena před kolektivem, který může zahrnovat několik desítek jedinců, ponížení oběti kyberšikany mohou v extrémních případech přihlížet statisíce i miliony (Rogers 2011,9; Szotkowski – Kopecký – Krejčí 2013, 27).

Šikaně lze často zabranit „pouhým“ odmítnutím tohoto chování jakožto nepřijatelného ze strany kolektivu či autorit. Zmíněný mechanismus v prostředí internetu často selhává z důvodů disinhibičního efektu. Přihlížející si ani nemusí být vědomi, že se stali svědky něčeho závažného (Chromý 2010, 43 – 44; Černá a kol. 2013, 24, 59-60).

Specifika kyberšikany lze shrnout do následujících bodů:

- Obětí se může stát kdokoliv;
- Možná anonymita agresora;
- Agresorem i obětí se může stát kdokoli;
- Nepřetržitý přístup k oběti;
- Kritérium opakování je naplněno publikováním;
- Široké publikum;
- Komplikovaná situace přihlížejících.

9.3 Specifika kyberšikany

Kybešikana zahrnuje široké spektrum agresivního chování různého rozsahu a závažnosti. V následujícím textu si ukážeme formy, s nimiž se setkáváme nejčastěji:

- Užívání cizí identity (imopersonation): agresor využívá přihlašovacích údajů oběti. Jménem své oběti jedná urážlivě s přáteli a známými oběti, kteří s ní následně mohou přerušit či omezit kontakt. Jako velmi nebezpečný způsob považuje J. Šmahaj *„zasílání útočných zpráv členům některé z nenávistných/ extrémních skupin (hate groups) s použitím jména, adresy, telefonu oběti.“* (Šmahaj 2014, 48).

- Vyloučení a ostrakizace (exclusion): záměrné vyloučení osoby ze skupiny komunikující prostřednictvím internetu. Mohou to být například skupiny sdružující se prostřednictvím sociálních sítí či online her a podobně. Vzhledem k potřebě mladých lidí někam patřit může být ostrakizace silně zraňující (Černá a kol. 2013, 25).

- Flaming: prudká hádka mezi dvěma i více účastníky. Flamming často probíhá v rámci různých diskusí a v chatovacích místnostech. Méně často je jako prostředek flamingu užíván e-mail. Toto jednání může přerůst v tzv. flame war. Útočník může spor zneužít a jeho části následně publikovat (Černá a kol. 2013; Šmahaj 2014,47).

- kyberharašení x kyberobtěžování (cyberharrasment): dlouhodobé zasílání zpráv urážlivého obsahu (Šmahaj 2014, 47). Rozdíl mezi kyberharašením a flamingem spočívá v jeho jednostrannosti. Oběť se do komunikace nezapojuje a není v jejích silách příval zpráv ze strany agresora ukončit (Černá a kol 2013, 26).

- Kyberstalking: oběť je pronásledována a vydírána. Na základě výhružek se cítí fyzicky ohrožena (Černá 2013 a kol, 26). Častou příčinou kyberstalkingu je nezvládnutí rozchodu jednou ze zúčastněných stran (Šmahaj 2014, 49). Od 1. 1. 2010 klasifikován je kyberstalking klasifikován jako trestný čin (Stotkowski – Kopecký – Krejčí 2013, 10).

- Očerňování, pomlouvání: šíření nepravdivých informací za účelem poškodit oběť. Kyberprostor může výrazně přispět k rychlosti a rozsahu šíření (Černá a kol. 2013, 27).

- Odhalení či outing: vyzrazení soukromých a citlivých informace, které agresor od oběti získal (Chromý 2010, 42; Černá a kol. 2013, 27).

- Happy Slapping: fyzické napadení oběti, které je zaznamenáno a posléze publikováno na internetu (Černá a kol. 2013, 25). Happy Slapping byl poprvé identifikován v Londýně v roce 2005. O tři roky později padly první rozsudky v kauze, kdy byl bezdomovec ubit skupinou adolescentů (Stotkowski – Kopecký – Krejčí 2013, 10).

Míra závažnosti se u jednotlivých útoků liší. Za nejzávažnější formy kyberšikany bývá považováno pořizování a zveřejňování fotografií a videí s cílem zesměšnit a ponížit oběť. Jako méně závažná formy je vnímán například Flamming. Pro posuzování je však vždy důležitý kontext (Černá a kol. 2013, 40).

K uvedeným druhům kyberšikany může docházet různými prostředky v různé míře a kombinaci. Agresoři k trýznění oběti užívají:

- Sociální sítě;
- Online interaktivní hry (MMORPG)
- Webové stránky;
- instant messengery;
- SMS a MMS;
- blogy;
- e-maily;
- chatovacích místnosti;
- internetové ankety a dotazníky (Černá a kol. 2013, 28-31).

9.4 Souvislost šikany a kyberšikany

Ačkoliv šikana a kyberšikana mohou existovat jako dva samostatné jevy, často spolu přímo souvisí. Mezinárodní výzkumy zaznamenaly řadu situací, v nichž internet představoval pouze další prostor pro útoky na osobu, která šikanu zažívá v offline světě (Price – Dalgleish 2010, 52). Ukázalo se, že až 85% obětí kyberšikany zažívá také tradiční formu šikany (Černá a kol 2013, 20).

Kyberšikana může být rozšířením tradiční šikany, kdy agresoři pronásledují svou oběť také prostřednictvím internetu. Zdánlivá anonymita internetu však nabízí i prostor pro odplatu. Šikanovaná oběť tak není limitována vlastní fyzickou silou, či nevýhodným postavením v kolektivu a může se agresorovi pomstít a stává se rovněž agresorem (Černá a kol. 2013, 31).

Narušené vztahy v offline světě se přenášejí rovněž do prostředí internetu a pronikají do komunikace prostřednictvím mobilních telefonů. Případy kyberšikany vyskytující se výhradně v prostředí moderních technologií patří k méně častým (Černá a kol. 2013, 20).

Vzhledem k tomu, že se větší část kyberšikany neodehrává na půdě školy, panují rozpory, jak v tomto případě postupovat. Může se stát, že škola odmítne problém řešit. To by však mohlo mít na celou situaci negativní dopad. Nepotrestání známého viníka představuje nebezpečný precedens, na základě kterého mohou být tyto aktivity později vyloženy jako přijatelné a hrozí další šíření kyberšikany (Černá a kol 2013, 99).

9.5 Důsledky kyberšikany

Badatelé se vesměs shodují že kyberšikana je stejně závažná jako šikana a má závažné emocionální a psychické důsledky (Šmahaj 2014, 43). Nejčastěji jsou zmiňovány tyto:

- *„Tenze, strach, stres;*
- *Změna self-konceptu oběti (sebevědomí, sebehodnocení, sebedůvěra, sebepojetí);*
- *Výskyt depresivních a neurotických obtíží;*
- *Časté poruchy spánku;*
- *Snížení frustrační tolerance;*
- *Pocit neřešitelnosti situace, ztráta životní pohody;*
- *Výskyt zkratovitého jednání, suicidální myšlenky;*
- *Zvyšující se bezdůvodná agrese a impulsivnost;*
- *Celková psychická nestabilita;*
- *Traumata a posttraumatická stresová porucha"* (Šmahaj 2014, 55).

V krajních případech může oběť přistoupit k sebevraždě (Šmahaj 2014, 43; Szotkowski – Kopecký – Krejčí 2013)

Zkušenost s kyberšikanou může rovněž ovlivnit vnímání a další užívání moderních technologií jak u obětí, tak u osob, které přihlížely. Obavy mohou přerůst v neadekvátní odmítání užívat internet a další moderní technologie. Jedinec se však tímto přístupem připravuje o četné výhody, které tyto technologie poskytují, zároveň riskuje sociální izolaci, neboť komunikace jejich prostřednictvím je v současnosti velmi rozšířena a u mladších generací se jedná takřka o samozřejmost (Černá a kol. 2013, 96). K obdobnému efektu může vést zákaz užívání internetu a dalších od rodičů (Černá a kol. 2013, 99). Vzniklá sociální izolace následně vede k dalším problémům.

Kyberšikana nemá dopad pouze na oběť. Skutky, kterých se agresoři dopouštějí, zanechávají leckdy stopy také na nich. To souvisí se skutečností, že agresivní chování se v mnoha případech obrací proti útočníkovi a ten se sám stává obětí. Kyberprostor tomu svými vlastnostmi napomáhá (Černá a kol. 2013, 92).

Jisté následky může kyberšikana vyvolat také u osob, které byly svědky útoku. Dosud není zcela jasné, jaký vliv na přihlížející má kyberšikana. Vzhledem k povaze internetu je možné, že negativní důsledky nemusí být tak časté a intenzivní (pamatujme však, že existuje mnoho způsobů kyberšikany s různou závažností!). Přesto mohou přihlížející kyberšikany pociťovat strach a bezmoc. Připomeňme, že zatímco u tradiční šikany jsou osoby se silným společenským statutem více chráněny, obětí kyberšikany se může stát každý. Přihlížení šikaně má však pozitivní vliv na osoby, které samy šikanu zažily. Vzniklá situace jim přináší poznání, že v tom nejsou sami (Černá a kol. 2013, 94). Nebezpečná situace ovšem nastává v okamžiku, kdy začne být šikana a s ní související kyberšikana považována v daném kolektivu za normu (Černá a kol. 2013, 97).

Kromě oběti, agresora a přihlížejících má kyberšikana negativní dopad na celý kolektiv (pokud je propojena s životem v offline světě), zasahuje rovněž do rodinného života oběti (Černá a kol. 2013, 96-99).

9.6 Řešení kyberšikany, obrana a prevence

9.6.1 Jak poznat oběť kyberšikany

Z výzkumů vyplývá, že pouze malé procento dospívajících se svěřilo s kyberšikanou rodičům, a to přesto, že jedinci, kteří kyberšikanu nezažili, uvádějí tuto možnost jako jednu z variant zvládání krizové situace (Černá a kol. 2013, 115, 117; Šmahaj 2014, 53). Jako důvody proč se rodičům nesvěřit obvykle uváděli obavy ze zamezení přístupu k internetu, strach z neporozumění, neznalost kyberprostředí ze strany rodičů a touhu vypořádat se s problémem sami.

Přesto lze odhalit změny v chování dítěte či mladistvého, které mohou indikovat tento problém:

- Změna ve vztahu k moderním komunikačním technologiím. Oběť může projevovat úzkost při práci s počítačem a mobilním telefonem. Jejich používání může omezit, či zcela odmítat.
- Oběť může pociťovat sklíčenost, časté jsou výkyvy nálad, ale také stavy apatie.
- Objevují se bolesti břicha, hlavy, nechutenství, nevolnost či problémy se spánkem.
- U obětí se často vyskytují také změny v chování k druhým. Mohou více vyhledávat samotu.
- U dětí a studentů můžeme pozorovat zhoršení prospěchu (Černá a kol. 2013, 52).

9.6.2 Technická řešení kyberšikany

Důležitým krokem je zamezit dalšímu přístupu agresora k oběti a minimalizovat vzniklé škody. Restriktivní opatření ovšem nepatří k nejvhodnějším způsobům. Navazování a rozvíjení vztahů má pro dospívající velký význam (Ševčíková 2014, 59). Zamezení přístupu k internetu – tedy k prostředí, které má výrazný podíl na socializaci dospívajících může zapříčinit sociální vyloučení a strádání (Ševčíková 2014, 59). Kyberšikanované dítě navíc nemusí mít přístup k internetu. Stačí, aby ho s vývojem situace seznámili například spolužáci (Černá a kol. 2013, 51).

Shrňme některé postupy, které je vhodné v tomto případě uplatnit:

- Oběť by měla vytvářet a uchovávat kopie útočných zpráv a projevů šikany – například s využitím klávesy Printscreen. Tyto záznamy mohou pomoci identifikovat a usvědčit viníka (Rogers 2011, 36).
- Dalším krokem je zablokování agresora. Většina stránek, které vyžadují registraci, umožňují blokovat konkrétní uživatele. Pokud mohou stránku užívat také neregistrovaní uživatelé, je třeba upravit přístup k účtu neregistrovaných uživatelů. Zablokování konkrétního uživatele umožňují také poskytovatelé emailových schránek.
- Vhodné je uvědomit administrátora. Administrátor může odstranit příspěvky se závadným obsahem či dokonce jejich autorovi zablokovat účet.
- V případě, že k obtěžování dochází prostřednictvím mobilního telefonu, je třeba zablokovat ve spolupráci s operátorem příslušné telefonní číslo.
- Pokud výše uvedená opatření nepomohou, další možností je založit si nové účty, e-mailovou schránku a telefonní číslo. Je vhodné využít dostupného zabezpečení a nové kontakty uvážlivě šířit.
- V případě odcizení přístupových údajů je nutné účet co nejdříve zablokovat.
- Pokud administrátor nereaguje, lze se obrátit na policii ČR (Černá a kol. 2013, 130-131).

Bohužel ne všechny formy kyberšikany lze zvládnout prostřednictvím technických řešení. Důležité je umožnit oběti podělit se o bolest a obavy. Na místě je situaci nepodcenit. Doporučována je také odborná psychologická péče, která může zmírnit negativní dopady kyberšikany (Černá a kol 2013, 124 - 125). Oběť může pociťovat bolest a hněv. Odplata však není konstruktivním řešením dané situace, neboť hrozí, že rovněž dosáhne měřítek kyberšikany. To by mohlo dotyčného vystavit dalším problémům (Rogers 2011, 36).

9.6.3 Kdy je vhodné kontaktovat policii

Kyberšikana spolu s šikanu pokládána za sociální deviaci. Pro srovnaní připomeňme, že za sociální deviaci je považována také kriminalita, toxikomanie či prostituce. Kyberšikana u nás není vnímána jako trestný čin, může však dosáhnout míry, kdy se stane trestněprávně postižitelnou (Chromý 2010, 41). K tomu dochází v následujících případech:

- Vydírání;
- Pomluva;
- Šíření pornografie;
- Výroba a jiné nakládání s dětskou pornografií;
- Zneužití dítěte k výrobě pornografie;
- Svádění;
- Šíření toxikomanie;
- Násilí proti skupině obyvatel a proti jednotlivci;
- Nebezpečné vyhrožování;
- Nebezpečné pronásledování (stalking);
- Hanobení národa, rasy, etnické nebo jiné skupiny osob;
- Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (Šmahaj 2014, 70).

9.6.4 Prevence kyberšikany

- Porozumět tomu jak kyberprostor funguje a jaká rizika se k němu váží;
- Dodržování pravidel bezpečného chování na internetu;
- Rodičovská mediace
    - Aktivní mediace zahrnuje společné sdílení činností na internetu, sdílení názorů a zážitků, umožňuje odhalit nenásilnou formou, jak se dítě v kyberprostoru orientuje a co ví o zásadách bezpečnosti (Černá a kol. 2013, 127);
    - Pasivní mediace spočívá v poučení o rizicích kyberprostoru, v poučení je potenciálních nebezpečích; a jak postupovat když se dostane do problémů (Černá a kol. 2013,127-128);
    - Sledování aktivit dítěte na internetu prostřednictvím zpětné kontroly, poté co ukončilo své aktivity;
    - Užití technologických aplikací limitující čas strávený na internetu.
- Dodržování pravidel bezpečného chování na internetu;
- Zvyšování kybernetické gramotnosti v rámci školní výuky (Černá a kol. 2013, 133);
- Školní programy zaměřené na problematiku kyberšikany a dalších online rizik (Černá a kol. 2013, 134).

Kontrolní otázky

Kdy se začal rozvíjet zájem o kyberšikanu?
Jaké druhy kyberšikany rozlišujeme a jakými prostředky k ní dochází?
Jaké technické prostředky lze využít, pokud ke kyberšikaně dojde?
Jak může kyberšikana souviset s šikanou?
Jaké kroky by měla učinit oběť kyberšikany?

Souhrn

Kyberšikana je závažné a opakované agresivní chování, jehož účelem je poškodit oběť. Má mnoho variant a dochází k ní různými prostředky. Badatelé se shodují, že následky kyberšikany mohou být velmi závažné. Je proto důležité tomuto chování předcházet zvyšováním obecného povědomí o tomto jevu.

Literatura a zajímavé odkazy

ROGERS, V. *Kyberšikana: Pracovní materiály pro učitele a žáky i studenty*. Praha:

Portál, 2011. 104 s. ISBN 978-80-7367-984-2

Publikace Vanessy Rogers z roku 2010 vyšla o rok později také v češtině. Přináší soubor cvičení zaměřených na problematiku kyberšikany, která jsou vhodná pro práci s dětským kolektivem.

ŠIMEK, P. a kol.: Co dělat, když… Praktické náměty k prevenci a intervenci krizového chování. Praha, 2010 – 2012. ISSN 1804-5537. Pracovní materiály jsou pravidelně aktualizovány.

Pro děti od 9 let a jejich rodiče je určena kniha Lenky Eckertové Hustej internet. ECKERTOVÁ, L.: Hustej internet. Praha: Petr Prchal Praha, 2014. 87 s. ISBN 978-80-87003-39-8.

V Brně každoročně probíhá konference Cyberspace kterou pořádá Ústav práv a technologií právnické fakulty ve spolupráci s Fakultou Sociálních studií Masarykovy university. Více informací najdete zde: http://cyberspace.muni.cz/.

Podívejte se také na:
www.e-bezpeci.cz
www.safeinternet.cz
www.stopcyberbullying.org
www.bezpecnyinternet.cz

10 Závěr

I když představuje internet opravdu multifunkční nástroj, je také plný hrozeb. Tyto hrozby pro uživatele znamenají někdy jen obtěžování a nutnost řešit obsazení počítače virem. Na druhou stranu ale také mohou přinášet spoustu problémů způsobených cílenými útoky, například ztrátu cenných dat, popřípadě různě velkého obnosu peněz.

Na druhou stranu internet nabízí i šíření buď samotných ochranných prostředků, nebo alespoň zvyšuje informovanost uživatelů o těchto. Ti se pak můžou rozhodnout, zda si pořídí některé z bezpečnostních řešení.

Cílem tohoto textu bylo tedy zejména přinést přehled o možných záškodnických i obranných technologiích. Zvláštní kapitola také patří hackerům. Tito lidé působící na internetu mohou přinášet další technologický rozvoj, neboť se o problematiku zajímají, někdy profesně, někdy ji berou jako koníček. Ve své podstatě, až na některé skupiny a jedince, kteří prosazují své zájmy, to jsou lidé, kteří rádi čerpají nové znalosti a prověřují je, i když někdy ne zcela legitimním způsobem.

Tyto tři skupiny, tedy škodlivý software, ochranné prostředky proti němu a hackeři, k internetu jako globální síti patří a neměli bychom je opomíjet.

Kromě výše uvedených rizik můžeme v kyberprostoru narazit na nebezpečí v podobě lidí, kteří se zde pohybují. Psychologické rysy kyberprostoru ovlivňují prožívání dějů, kterých se v kyberprostoru účastníme, a mají za následek opadání zábran, z čehož pramení určité druhy rizikového chování, které pomyslně vkládají zbraň do rukou potenciálních agresorů. Je proto třeba být si vědom potenciálních nebezpečí. Je proto nesmírně důležité zvyšovat povědomí o této problematice ve všech generacích, které se s internetem a kyberprostorem potkávají.

Přestože rizika užívaní internetu jsou poměrně závažná, není žádoucí propadat panice. Informační a komunikační technologie se staly nedílnou součástí našeho života a nám nezbývá, než se vyrovnat s hrozbami, která s sebou život přináší, ať už se s nimi setkáváme v offline či online světě.

11 Bibliografické odkazy

11.1 Literární zdroje

ČERNÁ, A. a kol. *Kyberšikana. Průvodce novým fenoménem.* Praha – Brno: Grada - Masarykova univerzita, 2013. 152 s. ISBN 978-80-247-4577-0.

D TEST: On-line podvody. dTest 4/2011, s. 40-41. ISSN: 9771210731015-04.

CHROMÝ, J. *Kriminalita páchaná na Mládeži. Aktuální jevy a nová právní úprava v České republice.* Praha: Linde Praha, 2010. 239 s. ISBN 978-80-7201-825-3.

HULANOVÁ, L. *Internetová kriminalita páchaná na dětech. Psychologie internetové oběti, pachatele a kriminality.* Praha – Kroměříž: Triton, 2012. 217 s. ISBN 978-80-7387-545-9.

JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.

OLWEUS, D. *Bullying at School. What we know and what we can do.* Oxford: Blackwell Publishers, 1994. 140 s. ISBN 0-631-19241-7.

POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, Policejní akademie České republiky v Praze. 2007. 219 s. ISBN 978-80-7251-250-8.

ROGERS, V. *Kyberšikana: Pracovní materiály pro učitele a žáky i studenty.* Praha: Portál, 2011. 104 s. ISBN 978-80-7367-984-2.

SZOTOWSKI, R. KOPECKÝ, K. KREJČÍ, V. *Nebezpečí internetové komunikace IV.* Olomouc: Univerzita Palackého v Olomouci, 2013. 177 s. ISBN 978-80-244-3911-2.

ŠEVČÍKOVÁ, A. a kol. Děti a dospívající online. *Vybraná rizikapoužívání internetu.* Praha - Brno: Grada Publishing – Masarykova univerzita, 2014. 184 s. ISBN 978-80-247-5010-1.

ŠMAHAJ, J. *Kyberšikana jako společenský problém.* Olomouc: Univerzita Palackého v Olomouci, 2014. 232 s. ISBN 978-80-244-4227-3.

11.2 Elektronické zdroje

AIR BANK. *10 dobrých rad pro bezpečné používání internetového bankovnictví.* [online] [23.4.2015] Air bank. 2013. Dostupné z WWW <https://www.airbank.cz/cs/vse-o-air-bank/novinky/10-rad-dobrych-rad-pro-bezpecne-pouzivani-internetoveho-bankovnictvi-v-pocitaci-ale-i-na-mobilu-nebo-tabletu/>

ALL ABOUT COOKIES. *Free cookie resources* [online] [cit. 2. 4. 2015]. All about cookies: [b.r.]. Dostupné z WWW: <http://www.allaboutcookies.org/cookies/>.

Antivirové centrum [online] [cit. 12. 4. 2015]. Antivirové centrum: ©1998-2015. Dostupné z WWW: <http://www.antivirovecentrum.cz/>.

APEK: *Pro spotřebitele* [online] [23.4.2015] APEK. Asociace pro elektronickou komerci. c2015. Dostupné z WWW <http://www.apek.cz/pro-spotrebitele/>

BELSEY, B. Cyberbullying: An Emerging Threat to the "Always On" Generation. [online] [10.4.2015] 2008. Dostupné z WWW <http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf>

BEZPEČNÝ INTERNET. [online] [cit. 5. 4. 2015]. Bezpečný internet: [b.r.]. Dostupné z WWW: <http://www.bezpecnyinternet.cz/>.

BINNARY, T. *Antivir*. [online] [cit. 1. 4. 2015]. ©2012. Dostupné z WWW: <http://www.guard-dynamics.cz/antivir>.

BITTO, O. *Trojské koně: co jsou zač a jak se bránit* [online][cit. 11. 4. 2015]. 2005. Dostupné z www:<http://www.zive.cz/clanky/trojske-kone-co-jsou-zac-a-jak-se-branit/sc-3-a-123708/default.aspx>.

BITTO, O. *Výběr antiviru: Které funkce potřebujete?* [online][cit. 18. 4. 2015]. 2011. Dostupné z WWW: <http://jnp.zive.cz/vyber-antiviru-ktere-funkce-potrebujete >.

BLOOMFIELD, H. *Mozilla Firefox Review* [online] [cit. 30. 4. 2015]. 2015a. Dostupné z WWW: <http://internet-browser-review.toptenreviews.com/mozilla-firefox-review.html>.

BLOOMFIELD, H. *Google Chrome Review* [online] [cit. 30. 4. 2015]. 2015b. Dostupné z WWW: <http://internet-browser-review.toptenreviews.com/google-chrome-review.html>.

BLOOMFIELD, H. *Opera Review* [online] [cit. 30. 4. 2015]. 2015c. Dostupné z WWW: <http://internet-browser-review.toptenreviews.com/opera-review.html>.

BLOOMFIELD, H. *Safari Review* [online] [cit. 30. 4. 2015]. 2015d. Dostupné z WWW: <http://internet-browser-review.toptenreviews.com/safari-review.html>.

BLOOMFIELD, H. *Internet Explorer Review* [online][cit. 30. 4. 2015]. 2015e. Dostupné z WWW: <http://internet-browser-review.toptenreviews.com/internet-explorer-review.html>.

BUŘÍNSKÁ, B. SVOBODA, J. *Stále více e-shopů chce za osobní odběr poplatek.* [online] [28.4.2015] 24.4.2013. Dostupné z WWW <http://www.novinky.cz/finance/299225-stale-vic-e-shopu-chce-za-osobni-odbery-poplatek.html>

CARLSEN, J. *Internet Browser Software Review* [online] [cit. 2. 4. 2015]. 2015. Dostupné z WWW: <http://internet-browser-review.toptenreviews.com/>.

CISCO. *What Is the Difference: Viruses, Worms, Trojans, and Bots?*[online][cit. 15. 3. 2015]. [b.r.]. Dostupné z WWW: <http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html#5>.

CKNOW. *Polymorphic viruses* [online] [cit. 15. 4. 2015]. 2013. Dostupné z WWW <http://www.cknow.com/cms/vtutor/polymorphic-viruses.html>.

COMPUTER HOPE. Free computer help and information[online][cit. 15. 4. 2015]. Computer hope: ©2015. Dostupné z WWW <http://www.computerhope.com/jargon/p/polyviru.htm>.

ČEPIČKA, D. a kol. *12 kroků pro bezpečnou komunikaci v sociálních sítích.* [online] [26.4.2015] PC World. 2013. Dostupné z WWW <http://pcworld.cz/internet/12-jednoduchych-kroku-pro-bezpecnou-komunikaci-v-socialnich-sitich-1-dil-45971>

ČESKÁ NÁRODNÍ BANKA. *Upozornění české národní banky na rizika spojená s využíváním elektronického bankovnictví.* [online] [23.4.2015] Česká národní banka. c2003 – 2015. Dostupné z WWW <http://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/upozorneni_el_bankovnictvi.html>

ČESKÁ SPOŘITELNA. *Platba s 3D Secure.* [online] [26.4.2015] Česká spořitelna. Dostupné z WWW <http://www.ivasekartapomuze.cz/banka/appmanager/portal/jpk?_nfpb=true&_pageLabel=jpk_doc&docid=internet/cs/sc_13340.xml>

ČMELÍK, M. *Seznamte se – DoS a DDoS útoky* [online] [cit. 16. 4. 2015]. 2013. Dostupné z www: <http://www.security-portal.cz/clanky/seznamte-se-%E2%80%93-dos-ddos-%C3%BAtoky>.

EVROPSKÉ SPOTŘEBITELSKÉ CENTRUM. *S čím vám můžeme pomoci?* [online] [23.4.2015] Evropské spotřebitelské centrum Česká republika. Dostupné z WWW <http://www.evropskyspotrebitel.cz/>

FIRETRUST. *About email viruses and worms* [online] [cit. 15. 4. 2015]. ©2015. Dostupné z WWW: <http://www.firetrust.com/products/benign/support/about_email_viruses_and_worms>.

F-SECURE. [online][cit. 8. 4. 2015]. F-secure: [b.r.]. Dostupné z www: <http://home.f-secure.com/en_global/>.

GET SAFE ONLINE. *Free expert advice.*[online] [cit. 3. 4. 2015]. Get safe online: ©2015. Dostupné z WWW: <https://www.getsafeonline.org/>.

GREENFIELD, P. YAN, Z. *Children, Adolescents, and the Internet: A New Field of Inquiry in Developmental Psychology*. [online] [20.4.2015] Developmental Psychology, vol. 42, No. 3, pg. 391 -394. 2006. Dostupné z WWW <http://www.apa.org/pubs/journals/releases/dev-423391.pdf>

HEUREKA BLOG: *Modrý, zlatý certifikát Ověřeno zákazníky, Garance nákupu… Jak se v tom orientovat?* [online] [23.4.2015] Heureka blog. 9.10.2013. Dostupné z WWW <http://blog.heureka.cz/modry-zlaty-certifikat-overeno-zakazniky-garance-nakupu-jak-se-v-tom-orientovat/>

HOAX. *Malware.* [online] [cit. 2. 4. 2015]. Hoax: ©2000-2015a. Dostupné z WWW: <http://www.hoax.cz/malware/>.

HOAX. *Co je phishing* [online] [cit. 2. 4. 2015]. Hoax: ©2000-2015b. Dostupné z WWW:<http://www.hoax.cz/phishing/co-je-to-phishing>.

HORÁK, V. *Úvod - Co je SPAM a jak se mu bránit.* [online] [cit. 5. 4. 2015]. 2006. Dostupné z WWW:<http://uvt1.cuni.cz/email/spam/uvod.html>.

IT slovník[online][cit. 6. 4. 2015]. IT slovník: ©2008-2015. Dostupné z WWW: <http://it-slovnik.cz/>.

ITBIZ. DDoS útok [online][cit. 6. 4. 2015]. [b.r.]. Dostupné z WWW: <http://www.itbiz.cz/slovnik/telekomunikace/ddos-utok>.

KARIERAWEB.CZ: Sociální sítě v pracovním procesu. [online] [23.4.2015] Karieraweb. 20.6.2011. Dostupné z WWW <http://kariera.ihned.cz/c1-52110270-socialni-site-v-pracovnim-procesu>

KASPERSKY LAB. Co je stealth virus? [online] [cit. 15. 4. 2015]. Kaspersky lab: ©1997-2015a. Dostupné z WWW: <http://www.kaspersky.com/cz/internet-security-center/definitions/stealth-virus>.

KASPERSKY LAB. Co to je trojský kůň? [online] [cit. 11. 4. 2015]. Kaspersky lab: ©1997-2015b. Dostupné z WWW: <http://www.kaspersky.com/cz/internet-security-center/threats/trojans>.

KASPERSKY LAB ZAO. Trojan-ArcBomb [online] [cit. 11. 4. 2015]. Kaspersky lab ZAO: ©1997-2015a. Dostupné z WWW: <http://securelist.com/threats/trojan-arcbomb/>.

KASPERSKY LAB ZAO. Trojan-Notifier[online][cit. 15. 4. 2015]. Kaspersky lab ZAO: ©1997-2015b. Dostupné z WWW:<http://securelist.com/threats/trojan-notifier/>.

KLUBAL, M. *Problematika sítí typu botnet.* [cit. 8. 4. 2015]. Brno: 2013. Dostupné z WWW (ke stažení): <http://is.mendelu.cz/zp/portal_zp.pl?prehled=vyhledavani;podrobnosti=55000;zp=37989;download_prace=1;lang=cz>.

KOLÁČEK, M. *Počítačová havěť - vývoj a rozdělení malware*. [online] [cit. 15. 4. 2015]. 2009. Dostupné z WWW:<http://www.svethardware.cz/pocitacova-havet-vyvoj-a-rozdeleni-malware/25680-3>.

KOZÁK, M. *Jak vytvořit opravdu silné heslo.* [online] [25.4.2015] Linuxepres. 2008.

Dostupné z WWW <http://www.linuxexpres.cz/praxe/jak-vytvorit-opravdu-silne-heslo>

KRČMA, P. *Jak (ne)bezpečné může být internetové bankovnictví?* [online] [23.4.2015] Computer world. Deník pro IT profesionály. 8.6.2012. Dostupné z WWW <http://computerworld.cz/securityworld/jak-ne-bezpecne-muze-byt-elektronicke-bankovnictvi-48497>

LIVINGSTON, S. HADDON, L. *Shrnutí projektu EU Kids online: Závěrečná zpráva.* [online] [15.4.2015] EU Kids online. 2009. Dostupné z WWW <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20%282006-9%29/EU%20Kids%20Online%20I%20Reports/cz_summary.pdf>

LIVINGSTON, S. HADDON, L. *Online dangers for children - report exposes the top 10 myths of internet safety.* [online] [cit. Datum] The London School of Economics and Political Sciece. 2011. Dostupné z WWW <http://www.lse.ac.uk/newsAndMedia/news/archives/2011/09/toptenmyths.aspx>

LUPA. *Jak zabezpečit počítač s Windows. Počítačoví červi a další havěť* [online][cit. 10. 4. 2015]. Lupa: ©1998-2015. Dostupné z WWW: <http://www.lupa.cz/specialy/jak-zabezpecit-pocitac-s-windows/pocitacovi-cervi-a-dalsi-havet/>.

MATĚJKA. *Stealth viry a anti-stealth techniky*. [online] [cit. 5. 4. 2015]. [b.r.]. Dostupné z WWW: <http://www1.osu.cz/home/matejka/soft/data/asthtech.htm>.

MASACHUSETS INSTITUTE OF TECHNOLOGY. *Viruses, spyware and Malware*. [online] [cit. 2. 4. 2015]. [b.r.]. Dostupné z WWW: <https://ist.mit.edu/security/malware>.

MEDIA GURU: *Sociální sítě: Twitter má v Česku nejmladší uživatele.* [online] [19.4.2015] Media Guru. 2015. Dostupné z WWW <http://www.mediaguru.cz/2015/04/socialni-site-twitter-ma-v-cesku-nejmladsi-uzivatele/#.VT1AcCG8PGd>

MIHALECH, M. *Niečo k problematike* DDoS[online-slovensky][cit. 6. 4. 2015]. Matěj Mihalech: ©2015. Dostupné z WWW: <http://www.shiba-inu.sk/matej/index.php?kap=protect>.

NOVÁKOVÁ, J. *Placení kartou po internetu je hračka. Rady pro bezpečné platby.* [online] [28.4.2015] Novinky.cz 2011. Dostupné z WWW <http://finance.idnes.cz/cesi-se-stale-trochu-boji-kartou-plati-jen-petina-f6s-/sporici-ucty.aspx?c=A111123_111851_viteze_sov>

PCRISK. *Adware*. [online] [cit.]. ©2015. Dostupné z WWW:<http://www.pcrisk.cz/adware>.

PETERKA, J. *Worm*. [online] [cit. 12. 4. 2015]. Computerworld 20/94, 1994. Dostupné z WWW: <http://www.earchiv.cz/a94/a420c120.php3>.

PETERKA, J. *Principy firewallů. Paketové filtry vs aplikační brány*. [online] [cit. 12. 4.

2015]. 2001. Dostupné z WWW: <http://www.earchiv.cz/b01/b0100024.php3>.

PŘIBYL, T. *Firewall: software nebo hardware.* [online] [cit.]. Online magazín ICT Security: ©2010. Dostupné z WWW: <http://www.ictsecurity.cz/odborne-clanky/firewall-software-nebo-hardware.html>.

PODNIKATEL.CZ. *E-shopystále častěji zneužívají loga certifikovaných obchodů, pozor na to.* [online] [28.4.2015] Podnikatel.cz. 2013. Dostupné z WWW <http://www.podnikatel.cz/clanky/e-shopy-stale-casteji-zneuzivaji-loga-certifikovanych-obchodu-pozor-na-to/>

PRÁVNÍ LINKA. *Pravidla při nákupu zboží přes internet [online] [20.4.2015] Právní linka.* 2014. Dostupné z WWW <http://www.pravnilinka.cz/bezplatna-pravni-poradna-zdarma/nakup-zbozi-pres-internet.html>

PRICE, M. DALGLEISH, J. *Cyberbullying: Experiences, impacts and coping as described by Australian young people.* [cit. 18.4.2015] Youth Studies Australia, 29, s. 51 – 59. 2010. Dostupné z WWW <http://www.kidshelp.com.au/upload/22882.pdf>

SKYBA, M. *Bezpečnost sociálních sítí.* [online] [cit. Datum] Norton. c1995 – 2015. Dostupné z WWW <http://cz.norton.com/social-networking-safety/article>

SSLS: *SSL certifikáty pro e-shopy.* [online] [24.4.2015] SSLS. c2006 – 2015. Dostupné z WWW <https://www.ssls.cz/eshopy.html>

Techopedia [online][cit. 18. 4. 2015]. Techopedia: ©2010-2015. Dostupné z WWW: <http://www.techopedia.com/>.

SULER, J. *The Basic Psychological Features of Cyberspace. Elements of a Cyberpsychology Model.* [online] [22.4.2015] The Psychology of Cyberspace. 1998. Dostupné z WWW <http://users.rider.edu/~suler/psycyber/basicfeat.html>

SULER, J. *The Online Disinhibition Effect* [online] [22.4.2015] The Psychology of Cyberspace. 2004. Dostupné z WWW <http://users.rider.edu/~suler/psycyber/disinhibit.html>

SZABÓ, F. *Bezpečnost dat na sociálních sítích.* [online] [cit. 26.4.2015] Affilblog. Listopad 2011. Dostupné z WWW <http://www.affilblog.cz/bezpecnost-dat-na-socialnich-sitich/>

TRAMPOTA, T. *Soukromí na sociálních sítích. Sociální sítě jako ukradené soukromí.* [online] [cit. 26.4.2015] Informační buletin 1. Úřad pro ochranu osobních údajů. 2013. s. 3-6. Dostupné z WWW <https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=4542>

TRUST PORT. Úvod do antivirové problematiky - Jak dělíme počítačové viry [online] [cit. 10. 4. 2015]. 2010. Dostupné z WWW:<http://www.trustport.com/manuals/antivirus/csy/techvirsdiv.htm>.

Webopedia[online][cit. 10. 4. 2015]. Webopedia: ©2015. Dostupné z WWW: <http://www.webopedia.com/>.

Wikipedie: otevřená encyklopedie[online][cit. 17. 4. 2015]. Wikipedie: [b.r.]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Hlavn%C3%AD_strana>.

12 Banka otázek

Součástí každého textu bude jako POSLEDNÍ KAPITOLA banka otázek. Uveďte, prosím, na tomto místě minimálně 50 otázek k tématu distančního textu s odpověďmi a, b, c, d – přičemž pouze 1 odpověď bude správná.

1. Replikace viru je schopnost
   a) infikovat počítač
   b) skrývat velikost souboru
   c) množit se
   d) upozornit uživatele na nákazu

2. Nákaza nerezidentními viry se šíří po
   a) stažení infikovaného souboru do počítače
   b) zadání příkazu v příkazové řádce
   c) zobrazení upozornění o této nákaze
   d) spuštění infikovaného souboru v počítači

3. Na sociálním inženýrství je založena
   a) schopnost manipulovat s uživatelem
   b) výuka a systém školení sociálních pracovníků
   c) manipulace a přerozdělování zdrojů
   d) aktivita stealth virů

4. Stealth vir při kontrole antivirovým programem
   a) přeruší spojení se serverem
   b) odhalí svou taktiku
   c) ukáže obsah souboru, který nakazil
   d) všechny uvedené možnosti

5. Polymorfní vir
   a) přepisuje původní algoritmus
   b) si zachovává původní algoritmus v každé kopii
   c) kopíruje algoritmus antivirového software
   d) ani jedna z možností

6. Notifier
   a) shromažďuje informace o počítači a jeho připojení k síti
   b) kryje záškodnické chování ostatního software
   c) vytváří proxy spojení
   d) zamezuje přihlášení do internetového bankovnictví

7. Rozdíl mezi DoS a DDoS útokem spočívá v
   a) signalizaci, kdy útok začne
   b) přístupu vně nebo zvenku sítě
   c) možnosti odhalení
   d) počtu zapojených počítačů

8. Počítače jsou zapojeny do botnetu
   a) registrací na webových stránkách
   b) po stažení speciálního software a jeho instalaci
   c) po nákaze trojským koněm, aniž o tom uživatel ví
   d) po instalaci antivirového software

9. Adware může mimo jiné také
   a) modifikovat nastavení webového prohlížeče
   b) blokovat vyskakovací okna
   c) bránit proti škodlivému software
   d) modifkovat data na nakaženém počítači

10. SPAM je
   a) nevyžádaná emailová zpráva s reklamním sdělením
   b) vyžádaná emailová zpráva s reklamním sdělením
   c) informační zpráva s obsahem kulturních novinek
   d) zpráva o stavu počítače zasílaná tvůrci operačního systému

11. Při spoofingovém útoku dochází
   a) k vytvoření botnetu
   b) k záměně identity, popřípadě adresy
   c) k rozesílání emailů na všechny adresy v kontaktech
   d) ke sledování stisknutých kláves

12. Hackeři uznávají jako autoritu
   a) script-kiddies
   b) odborníky v oboru
   c) parlament
   d) programátory

13. White hats hackeři
   a) posuzují činnost ostatních hackerů
   b) provádějí průmyslovou špionáž
   c) nevyužívají svých znalostí pro vlastní obohacení
   d) neuznávají morální principy

14. Antivirový systém poskytuje
   a) ochranu jen před určitými druhy virů
   b) komplexní antivirovou ochranu
   c) ochranu jen na vyžádání
   d) informace o zavirovaných počítačích v síti

15. White list
   a) využívají white hats hackeři
   b) obsahuje seznam navštívených webů
   c) využívá antivir jako karanténu
   d) obsahuje soubory, které antivirus nemusí kontrolovat

16. Citlivost heuristické analýzy
    a) závisí na nastavení uživatelem
    b) se mění v závislosti na délce skenování
    c) závisí na počtu spuštěných rezidentních štítů
    d) ovlivňuje test integrity

17. Služba VirusTotal
    a) přináší informace o nových trojských koních
    b) slouží jako prevence pharmingu
    c) je využívána hackery ke kompletnímu zavirování počítače
    d) slouží k online testování souborů a webových adres

18. Hardwarový firewall
    a) má rozšířenější možnosti správy než softwarový
    b) je spojení hardware a specializovaného software pro ochranu počítačové sítě
    c) má nízké pořizovací náklady
    d) nabízí další doplňkové služby

19. Aktualizace software jsou důležité z důvodu
    a) odladění chyb pomocí různých záplat a oprav
    b) obsazení pevného disku daty
    c) sledování činnosti na počítači
    d) informování uživatele o novinkách ve vývoji

20. Nejstarším používaným webovým prohlížečem je
    a) Mozilla Firefox
    b) Internet Explorer
    c) Opera
    d) Safari

21. Mozilla Firefox nemá tuto funkci
    a) synchronizace s účtem Google
    b) rodičovskou kontrolu
    c) zobrazení PDF souboru
    d) mazání cookies

22. Webový prohlížeč slouží
    a) ke kontrole nainstalovaných her v počítači
    b) k získání přehledu činnosti, kterou na počítači provádí jiný uživatel
    c) k vytváření obsahu webové stránky
    d) k zobrazování obsahu webových stránek

23. Opera
    a) má jednoduché ovládání
    b) má široké možnosti technické podpory
    c) nemá napoprvé tak jednoduché ovládání
    d) neumožňuje využívání klávesových zkratek

24. Internet Explorer
    a) je dodáván s operačním systémem Linux
    b) není téměř známý
    c) je integrován do operačního systému Windows
    d) neumožňuje dotykové ovládání

25. Cookies jsou informace o
    a) počtu antivirových kontrol na vyžádání uživatelem
    b) navštívených webových stránkách
    c) uživatelských účtech na počítači
    d) bezpečnou možností přihlášení do internetového bankovnictví

26. Asociace pro elektronickou komerci uděluje certifikát
    a) Garance nákupu
    b) APEK
    c) Ověřeno zákazníky
    d) Záruka kvality

27. K placení na internetu není vyžadováno
    a) Datum expirace karty
    b) Číslo karty
    c) Pin
    d) CVV/CVC kód

28. Zákazník má při nákupu na dálku ze zákona nárok odstoupit od smlouvy:
    a) Ano
    b) Ne
    c) Ne, pokud si tuto službu nepředplatil
    d) Ano, ale netýká se to vybraných druhů zboží

29. Webcamtrolling je
    a) Nástroj pro zlepšení funkce webkamery
    b) Přátelská komunikace prostřednictvím webkamery
    c) Užití klamavé videosmyčky simulující webkameru
    d) Program pro úpravu videí

30. Disinhibiční efekt způsobuje
    e) Větší zdrženlivost
    f) Úzkostné stavy
    g) Opadnutí zábran
    h) Svalové křeče

31. MMORPG je zkratka označující
    a) Typ online počítačových her
    b) Sociální síť
    c) Webový prohlížeč
    d) Patologické chování

32. Digital divide je:
    a) Důsledek rizikového chování v kyberprostoru
    b) Dopad kyberprostoru na mladou generaci
    c) Generační propast způsobená odlišným přístupem ICT mezi dvěma generacemi
    d) Výraz používaný hráči online her

33. Always on je termín užívaný v souvislosti s:
    a) Generací narozenou po roce 1994
    b) Známou hackerskou skupinou
    c) Označení jedinců závislých na internetu
    d) Druh internetového připojení

34. Lze tvrdit, že anonymita v kyberprostoru je
    a) Absolutní
    b) Vnímána subjektivně
    c) Snadno dosažitelná
    d) Škodlivá

35. Sociální sítě neslouží
    a) K sdružování
    b) Ke sdílení fotografií a videí
    c) K anonymnímu přispívání do diskusí
    d) K vytváření sociálních skupin

36. Mirroring je
    a) Technika ochrany počítače
    b) Způsob manipulace hojně užívaný kybergroomery
    c) Aplikace na sociálních sítích
    d) Online počítačová hra

37. Sexting je
    a) Pořizování a následné zveřejnění a šíření textu, fotografií a videí se sexuální tématikou
    b) záměrné šíření dětské pornografie
    c) forma kyberšikany
    d) Trestný čin

38. Kybergooming nezahrnuje:
    a) Hovory na téma sexuality
    b) Manipulace s obětí
    c) Falešnou identitu predátora
    d) Krádež

39. Větší pozornost je kyberšikaně je ve světě věnována:
    a) Od 80. let 20. Století
    b) Od 90. let 20. století
    c) Po roce 2000
    d) Od roku 2010

40. Autorem termínu kyberšikana je
    a) Dan Olweus
    b) John Dalgleish
    c) Sonia Livingston
    d) Bill Belsey

41. Kyberšikana se od tradiční šikany liší
    a) Opakovaným chováním
    b) Agresivním chováním se záměrem poškodit oběť
    c) Nerovnoměrností rozložení sil mezi obětí a agresorem
    d) Využitím ICT

42. Mezi druhy kyberšikany nepatří:
    a) Happy Slapping
    b) Kyberharašení
    c) Stalking
    d) Kyberhádka

43. Flamming je
    a) Způsob ochrany přihlašovacích údajů
    b) Prudká hádka mezi účastníky diskusí a chatů
    c) Strategie zvládání stresu
    d) Pronásledování oběti

44. Pořízení a zveřejnění záznamu fyzického napadení oběti označujeme za
    a) Flamewar
    b) Kyberstalking
    c) Happy Slapping
    d) Kyberobtěžování

45. Pod pojmem outing rozumíme
    a) Prozrazení důvěrné informace o oběti osobě, které nebyla určena s cílem oběť poškodit
    b) Veřejné přiznání homosexuální orientace
    c) Nepřiměřené odhalování citů
    d) Způsob ochrany soukromí

46. Mezi vhodná řešení kyberšikany nepatří

a) Zákaz přístupu k internetu a dalším moderním technologiím
b) Svěřit se osobě, ke které máme důvěru
c) Přijmutí technických opatření
d) Vyhledání odborné pomoci

47. Kyberšikana může závažným způsobem zasáhnout do života:
a) Oběti
b) Přihlížejícího
c) Agresora
d) Všech zúčastněných

48. Mezi technická řešení kyberšikany nepatří
a) Blokování agresora
b) Kontaktování administrátora
c) Založení nového účtu či změna čísla
d) Střet s agresorem

49. Dobře zvládnutá rodičovská mediace nespočívá v
a) Sdílení online aktivit s potomkem a povídání si o zkušenostech s online světem
b) Sledování aktivit dětí a mladistvých na internetu
c) Regulování času, který potomek tráví na internetu
d) Zákaz užívání moderních technologií, protože je to zbytečnost a ztráta času

50. Prevencí kyberšikany není
a) Dodržování pravidel bezpečnosti
b) Odmítavý přístup
c) Zvyšování kybernetické gramotnosti
d) Sledování aktivit dítěte na internetu