Útok z internetu na vaše PC

IRC/ICQ/Jabber/WebChat/e-mail/P2P – bavte se na internetu s co nejmenším rizikem

MARTIN IGNJATOVIČ

Nejen svou prací je člověk živ, a tak spousta uživatelů používá svůj počítač i pro zábavu. Hlavní zábavou na počítačových systémech jsou počítačové hry, avšak ty nejsou hlavním tématem tohto článku. My si povíme o zábavě v síti internet a podíváme se především na rizika, která z ní plynou. Nebudeme zacházet do velkých technických detailů – spíše se pokusíme obecně poradit a pojmenovat rizika.

IRC

IRC (Internet Relay Chat) je rozšířen hlavně mezi pokročilejšími uživateli, a zejména mezi uživateli systémů UNIX, Linux. Jeho koncepce je velmi stará, nicméně stále oblíbená a zdokonalovaná. Nejde o IM jako u ICQ, ale o rozhovor více uživatelů (klasický chat). První, co k používání IRC musíte mít, je klientský program. Těch jsou opět desítky, ale mezi nejpopulárnější na platformě Windows patří mIRC. U unixových systémů záleží na každém uživateli, kterému klientskému programu dá přednost, na výběr je jich opravdu hodně. Jmenujme alespoň některé – BitchX, Ksirc, Xchat, Irssi atd. Další věcí, kterou musíme znát, je adresa serveru, k němuž se chceme připojit. Většina moderních klientů přichází s vestavěným seznamem světových IRC serverů.

Uživatelé v Česku nejspíš využijí služeb nejznámějších českých IRC serverů, k nimž patří například *irc.felk.cvut.cz*, *irc.i.cz* atd. Důležitá u serveru je rovněž znalost portu, na kterém server naslouchá. U většiny serverů jsou to porty 6666–6667, ale existují i servery, které naslouchají na portech 80 nebo 443 (irc.i.cz), což ocení zejména uživatelé schovaní na firewallem. Základem IRC nejsou rovněž nějaké stránky nebo klikací utility, ale příkazy, jimiž se klientský program ovládá. Seznam těchto příkazů a dalších rad a návodů najdete na stránkách *www.irc.cz*. Mezi další vlastnosti patří přenos souborů nebo soukromý chat. Pokud vytvoříte vlastní místnost, stáváte se zpravidla jejím správcem, jenž má možnosti mnohem větší než uživatel, který se k chatu připojí.

▲ Uživatelé v Čechách nejspíš využijí služeb nejznámějších českých IRC serverů, k nimž patří např. irc.felk.cvut.cz.

RIZIKA: Rizik číhajících na uživatele na IRC je opravdu mnoho. Každodenní války různých crackerských a hackerských skupin jsou tu na denním pořádku, takže se není čemu divit, pokud to občas odnesou i nevinní „civilisté". Ti se zpravidla stávají bez svého vědomí prostředkem k útoku na další systém. Rovněž se zde najdou různí škodolibí uživatelé, kteří se baví tím, že útočí na klientské systémy. Je to dáno hlavně tím, že zjistit IP adresu klienta není vcelku problém. Další nebezpečí hrozí rovněž od různých automatizovaných skriptů, jež mohou napadat klientský program či počítač. Šíření nelegálního obsahu (software, video, hry, audio) je také poměrně časté, a ne každý soubor musí být opravdu tím, co požadujete.

OPATŘENÍ: Nyní již k opatřením na obranu. Vždy si zajistěte, aby váš klientský program byl aktualizovaný. Např. v programu mIRC je objevena bezpečnostní chyba každou chvilkou. Rovněž dobře zabezpečte a aktualizujte svůj systém (tato rada neplatí jen pro IRC). Máte-li na výběr, používejte server, který vám zajistí anonymní přístup, aby nebyla zjistitelná vaše IP adresa. Pokud stahujete software přes IRC, nevěřte slepě názvu souboru, ale proveďte testy (antivirem atd.). Podobně jako u ICQ nevěřte lidem, které neznáte.

ICQ

ICQ je jedním z nejpopulárnějších IM (Instant Messaging) systémů. Používají ho miliony uživatelů po celém světě. Umožňuje toho opravdu mnoho. K popularizaci toho systému přispěla jistě jeho koncepce. Ta je založena na jedinečném číselném identifikátoru, takzvaném UIN. UIN má každý uživatel tohoto systému jedinečné a dá se přirovnat k telefonnímu číslu. Dva uživatelé nemohou mít stejné UIN, přezdívku, pod kterou vystupují, však ano. Centrem všech uživatelů ICQ jsou domovské stránky projektu, jež naleznete na adrese *www.icq.com*. Zde si můžete založit své konto, ovládat ho, hledat ostatní uživatele, zanechávat jim vzkazy a spoustu jiných věcí. Lze si zde samozřejmě bezplatně stáhnout i klientskou část systému, pomocí níž můžete komunikovat s ostatními uživateli. Klientských programů existuje velice mnoho. Patrně nejpoužívanější jsou klienty ICQ Pro 200x a ICQ Lite. ICQ Pro je oficiální klientský program a poskytuje podporu všech vlastností, které systém nabízí. ICQ Lite je pak jeho odlehčená verze. Populární jsou rovněž programy třetích stran. Klientské programy existují i pro ostatní platformy, jako například LICQ nebo MICQ pro *nixové systémy. Co vlastně ICQ nabízí? Asi nezákladnější a nejznámější funkcí systému je posílání zpráv ostatním uživatelům. Zprávu můžete poslat jakémukoliv uživateli, jehož UIN znáte. Máte rovněž možnost si uživatele, se kterými komunikujete, často přidat do svého Contact Listu. Tak rovněž poznáte, zdali je daný uživatel on-line či ne. K přidání uživatele do Contact Listu zpravidla potřebujete jeho svolení (autorizaci). Systém dále nabízí možnost rozhovoru více uživatelů (chat), posílání souborů, SMS, e-mailů a mnoho dalších. Nyní se podíváme na rizika, která tento systém přináší, a povíme si o opatřeních, jimiž lze tato rizika minimalizovat.

RIZIKA: Mezi první rizika, se kterými se můžeme u ICQ setkat, je příjem nevyžádaných zpráv. Ty jsou rozesílány pomocí automatizovaných nástrojů, které generují klientská UIN, a na ty pak posílají různé odkazy a zprávy. Nejčastěji se jedná o reklamu nebo odkazy na pornografické a podobné stránky. Dalším rizikem, se kterým se můžeme setkat, jsou útoky na klienta ICQ nebo dokonce na počítač, na kterém klient běží. K úspěšnému provedení tohoto útoku potřebuje znát útočník IP adresu daného stroje. Rozšířeným nešvarem je rovněž zneužívání důvěry ostatních uživatelů a rozesílání souborů s nebezpečným obsahem (viry, backdoory, trojské koně atd.). Nyní se podíváme na to, jak lze takovým rizikům předejít.

▲ CQ je jedním z nejpopulárnějších instant messaging systémů.

OPATŘENÍ: Klientské programy ICQ obsahují zpravidla nástroje, jimiž lze výše uvedená rizika eliminovat. Zabránit příjmu nevyžádaných zpráv lze celkem snadno v nastavení klienta, kde zvolíme, že nechceme přijímat zprávy z webového komunikačního centra, z e-mailového centra. Můžeme dokonce zvolit možnost, že nechceme přijímat zprávy od uživatelů, kteří nejsou v našem Contact listu, což je velmi užitečná vlastnost. Identifikaci našeho systému podle IP adresy lze rovněž zabránit tak, že zakážeme zobrazovat naši IP adresu.

Pozor, tato možnost nás neochrání v případě, že chceme někomu poslat nebo od někoho přijmout nějaký soubor. Poté již zjištění IP adresy našeho systému nic nebrání. Pokud tuto možnost zvolíte, jsou všechny zprávy posílány přes server systému ICQ. Rovněž doporučuji zapnout. Obrana před soubory se škodlivým obsahem není jednoduchá.

Zde pomůže snad jen vaše obezřetnost. Pokud člověka, se kterým si píšete, dobře neznáte, raději od něj žádné soubory nepřijímejte, hlavně ne soubory spustitelné (exe, vbs, atd.), i kdyby vám váš protějšek tvrdil, jak je takový soubor skvělý a ať jej určitě zkusíte. Zneužívání důvěry patří mezi nejčastější útoky na systémy jednotlivých uživatelů.

▲ Jabber je založen na otevřeném zdrojovém kódu a XML.

Jabber

Jabber je mohutně se rozvíjející IM systém. Je založen na otevřeném zdrojovém kódu a technologii XML. To jej činí velmi populárním a je nasazován i jako podnikový IM systém. Instalace jabber serveru je velmi jednoduchá. Zdrojové kódy získáte na adrese *www.jabber.org*. Rovněž konfigurace serveru je velmi snadná a provádí se pomocí souboru jabber.xml. Tento soubor je velmi dobře okomentovaný, a není tudíž problém nastavit si jabber podle svých představ. K jabberu existují rovněž i přídavné moduly. Nejpoužívanější jsou jistě konference a jud (jabber users directory). Modul konference umožňuje komunikaci více uživatelů najednou (chat) a modul jud umožňuje vyhledávat uživatele a informace o nich. V neposlední řadě je výhodou jabberu také to, že podporuje SSL. O tom až za chvíli. K připojení potřebujete dvě věci. Jednou z nich je klientský program a druhou server. Klientských programů je opět mnoho, nejlepším na platformě Windows je patrně JAJC či Exodus. Pod *nixovými systémy jsou pak populární PSI, Gabber a další. Čeští uživatelé dají zřejmě přednost serveru *jabber.cz*. Toto však nejsou všechny funkce, které jabber podporuje. Obsahuje i podporu pro ICQ, AIM a další, takže pomocí jednoho klienta můžete komunikovat s uživateli výše zmíněných služeb. Pod-

mínkou je, aby tyto služby podporoval vámi vybraný server. Jinak lze pomocí jabberu dělat standardní věci, jako vést rozhovor, posílat zprávy a soubory. Uživatelé jsou identifikováni pomocí svého nick name, což je vzhledem k ICQ určitá nevýhoda. Na druhou stanu nemohou existovat dva uživatelé na jednom serveru se stejným nick name. Nyní již k rizikům jabberu.

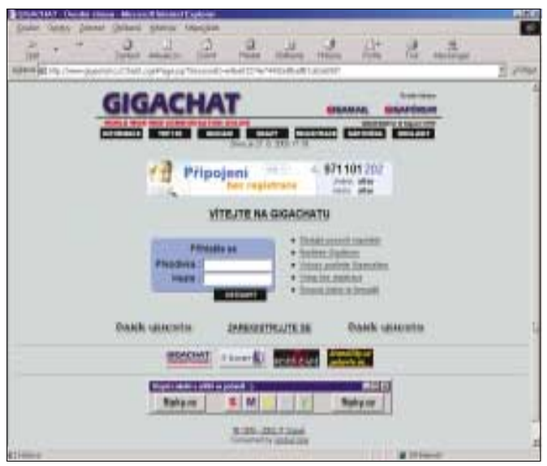
RIZIKA: S možnostmi, které jabber nabízí, roste i riziko zneužití. Naštěstí je vše založeno na otevřeném zdrojovém kódu, takže většina chyb je velmi rychle odhalena a opravena. U jabberu hrozí podobná rizika jako u ICQ, a bránit se proti nim lze podobně. Pokud váš server podporuje SSL, určitě jej použijte, protože odposlouchávat komunikaci pomocí různých snifferů není opravdu žádný problém a data jsou velmi snadno čitelná, díky formátu XML.

OPATŘENÍ: Podobně jako u ICQ nastavte bezpečnostní opatření na maximální možnou míru, dodržujte elementární bezpečnostní zásady a nedůvěřujte slepě cizím lidem. Aktualizace klientských programů a systému jsou opět namístě. Pokud je jabber provozován jako váš podnikový IM systém, mějte na paměti, že vaše data mohou být sledovaná (pokud není použito SSL) a historie zpráv zůstává ve vašem systému. Pokud si toto uvědomíte, předejdete tak mnoha nepříjemnostem.

Web Chat

Webové chaty patří k nejpopulárnějším druhům komunikace mezi uživateli. K jejich využívání nepotřebujete krom webového prohlížeče nic. Je to velmi výhodné v případě, kdy používáte několik systémů a nechce se vám na každý z nich instalovat komunikačního klienta. Webových chatů jsou po síti miliony. Jejich tvorbu zvládne téměř každý programátor, který se zabývá tvorbou webových aplikací. Existují však velké chaty na specializovaných serverech, kde jsou registrovány tisíce uživatelů. Tyto chaty zpravidla neposkytují takové možnosti jako ostatní systémy (výměna souborů atd.), ale nebezpečí zde číhá také. Podíváme se jaké.

RIZIKA: Rizika, která na nás číhají na web chatu, se mohou lišit a to zejména v závislosti na tom, jaké možnosti chat poskytuje. Jednoduché chaty, jež krom psaní zpráv neumožňují téměř nic, lze označit za poměrně bezpečné, i když ani zde není vyloučena možnost, že někdo objeví bezpečnostní nedostatek systému a ten pak využije ve svůj prospěch. Daleko nebezpečnější jsou špatně (občas záměrně) zabezpečené chaty, jež umožňují interpretaci kódu. Pro zkušeného útočníka pak není problém vložit do svého příspěvku kus škodlivého kódu, který tak může například shodit webový prohlížeč všech uživatelů připojených k této konkrétní stránce. Takovýto škodlivý kód lze aplikovat na aktuální bezpečnostní nedostatky konkrétního prohlížeče a může vést až ke kompromitaci celého systému.



▲ **Webové chaty patří k nejpopulárnějším druhům komunikace mezi uživateli.**

OPATŘENÍ: Opatření jsou celkem snadná. Vždy mějte aktualizovaný prohlížeč i systém. Dobře si vyberte server, na kterém budete chatovat, a zjistěte si co vše nabízí. Pokud server zobrazuje IP adresy klientských počítačů, měli byste se takovému serveru vyhnout. Rovněž server, který po vás vyžaduje zadání osobních údajů, nepůsobí příliš důvěryhodně (údaje lze samozřejmě zadat falešné).

E-mail

E-mail používá dnes prakticky každý. Je to nejrozšířenější prostředek komunikace mezi uživateli. Vysvětlování principů a možností by bylo nošením dříví do lesa, a proto se rovnou podíváme na nebezpečí, které nám přes e-mail hrozí.

RIZIKA: Rizika e-mailu jsou všeobecně známá. Nejčastěji jde o šíření virů, červů a spamu. Bohužel i přes známost těchto rizik a známost protiopatření je e-mail nejčastěji používaným prostředkem pro šíření výše uvedených věcí.

OPATŘENÍ: Opatření proti virům a červům jsou jednoduchá, a je až s podivem, že se jim v prostředí sítě tolik daří. Zde je uvedeno několik zásad, které vás v 90 procentech případů ochrání před viry a červy.

- aktualizovaný systém
- aktualizovaný poštovní klient
- aktualizovaný antivirový program
- mazání e-mailů s neznámým obsahem
- neotevírání příloh s podezřelým obsahem

Jednoduché, že? Bohužel většina uživatelů nedodržuje často ani jeden z předchozích bodů, a velmi výrazně tak přispívá k šíření této elektronické „havěti".

Obrana proti spamu (nevyžádané poště) tak jednoduchá není a nevyžádaná pošta je noční můrou většiny systémových administrátorů. Pro domácí uživatele, kteří jsou správci svého systému, lze uvést několik zásadních doporučení, jež nebezpečí spamu výrazně eliminují. Tato opatření platí pro případ, že spamem ještě nejste postiženi. Pokud ano, cesta zpět není snadná.

Základním pravidlem je nezveřejňovat svou e-mailovou adresu. Založte si další e-mailovou adresu a tu pak zveřejňujte, třeba při různých registracích, v konferencích atd. Tato adresa by měla být jakousi náhradou. Soukromou adresu používejte opravdu jen soukromě. Bohužel ani to vám nezaručí bezpečí, protože může být tato adresa získána z každého systému, kde je uložena. Rovněž sledování síťového provozu může být pro spamery svatým grálem. Také různé roboty, které prohledávají webové stránky, jsou užitečným zdrojem pro rozesílatele spamu. Pokud se vám i tak stane, že jste zařazen do nějaké databáze a je vám doručována nevyžádaná pošta, máte ještě naději na záchranu. Existují nástroje, pomocí kterých se lze bránit. Například webový prohlížeč Mozilla, respektive její e-mailový klient, má v sobě integrovanou ochranu proti spamu a tato ochrana funguje poměrně spolehlivě. Existují i další programky a utility, a záleží jen na vás, které vám budou vyhovovat. Ale i tak je zatěžována vaše přenosová linka. Ochrana proti spamu není vůbec snadná a eliminovat jeho rizika je prakticky nemožné. Pomohla by snad nějaká celosvětová kampaň, ale to je zatím spíše utopie.

▲ **E-mail je nejčastěji používaným prostředkem pro šíření virů, červů a spamu.**

P2P

Výměnné systémy peer-to-peer jsou poslední dobou velmi diskutované. Jde zejména o sdílení nelegálního softwaru, videa, hudby a her. Lze zde však najít i velké množství legálních dat, a proto není důvod takové systémy zcela zavrhnout. Tyto systémy jsou navzdory právním sporům, žalobám a výhružkám různých společností stále populárnější. Nejznámější P2P systémy jsou DirectConnect a Kazaa. Existují i produkty dalších společností, ale tyto dva jsou nejrozšířenější. Nebezpečí, které na těchto systémech existuje, je však velmi vysoké.

RIZIKA: Rizika, která na nás čekají v sítích P2P, jsou značná. Nejenže jejich používáním riskujete žalobu od nějaké společnosti zabývající se ochranou autorských práv (BSA, RIAA atd.), což většinu uživatelů stejně neodradí, ale daleko nebezpečnější je možnost kompromitace systému. Po takovýchto sítích mohou kolovat různé červy, viry atd. Pokud nějaká data stahujete, nikdo vám nezaručí jejich původ a pravost.

OPATŘENÍ: Rozhodnete-li se nějaký systém P2P používat, dodržujte bezpečnostní opatření. Pokud bezpodmínečně nemusíte, zakažte sdílení dalším uživatelům. Tím nejenže ušetříte svou přenosovou kapacitu, ale zároveň zavřete část vrátek do vašeho systému. Stažené soubory pak důkladně testujte antivirovými a podobnými programy, a nevěřte bezhlavě jejich obsahu. Svůj systém i klientský program udržujte aktualizované.

▲ **P2P systémy jsou navzdory všem právním sporům, žalobám a výhružkám různých společností stále populárnější.**

Nápady, dotazy, návrhy témat, jež vás zajímají a připomínky zasílejte na adresu igm@centrum.cz. Na vaše dotazy k této problematice se pokusíme najít odpovědi. 3 0523/FEL ❑