INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Michal Moc

Bezpečné užívání internetu

Metodická příručka

Ing. Michal Moc

Bezpečné užívání internetu

Vydalo Centrum pro studium vysokého školství, v.v.i. , Praha, 2015

Návrh obálky Radka Šebková

Publikace vznikla jako výsledek projektu Věda pro život, život pro vědu (VĚŽ).
Projekt byl řešen v rámci operačního programu Vzdělávání pro konkurenceschopnost, prioritní osa Terciární vzdělávání, výzkum a vývoj, v období březen 2014 až červen 2015.
Číslo projektu: CZ.1.07/2.3.00/45.00 29

ISBN 978-80-86302-77-5

Bezpečné užívání internetu

1 Úvod

1.1 Internet – základní pojmy

Nejprve si budeme muset definovat základní pojmy, které budeme potřebovat v následujících kapitolách.

- Server je počítač nebo také skupina počítačů poskytující nějakou službu.
- Klient může být počítač, mobil, tablet či jakákoliv aplikace, která využívá služeb serveru.
- Protokol je definovaný způsob komunikace mezi serverem a klientem.

Pokud máme definovány tyto tři základní pojmy, pak můžeme prohlásit, že na internetu nám vždy probíhá nějaká komunikace mezi klientem a serverem.

1.2 Internet – principy

Každé přímo připojené zařízení do sítě internetu má svoji IP adresu[1]. Nejčastěji se setkáváme s IP adresami verze 4. Jedná se o čtyři sady čísel v rozsahu 0 až 255, jak můžeme vidět na následujících ukázkách:

www.google.com = 74.125.87.99,
www.isste.cz = 77.104.223.229,
www.fjfidecin.cz = 77.95.47.98.

Adresy verze 4 můžeme ještě rozdělit na lokální a globální. To je z toho důvodu, aby nám jejich rozsah taj rychle nedošel. Většinou je to zařízeno tak, že třeba školní síť nebo vaše síť doma používá lokální adresy, které připojeným zařízením rozdává router. Je jedno, jestli jsou zařízení připojena přes WiFi nebo kabelem. Jak už jsme si řekli na začátku, každé zařízení

[1] IP adresa je číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, které používá IP (internetový protokol).

musí dostat IP adresu. Domácí nebo školní síť vám přidělí adresu z jejího rozsahu. Nejčastěji 192.168.x.x, kde x může nabývat hodnot 0 až 255. Samozřejmě, že se dají i adresy přidělovat „natvrdo“, ale je lepší to nechat na DHCP[2] serveru (běží v routeru). Díky tomuto mechanismu pak stačí, aby váš domov nebo škola měly pouze jednu veřejnou IP adresu pro router a dále už je jedno, kolik zařízení je připojeno ve vnitřní síti.

Možná už jste si na internetu nebo v novinách přečetli, že hrozí konec nebo jenom kolaps internetu, protože dojdou adresy verze 4. Ano, to je pravda. Ale pouze to, že dojdou tyto adresy. Protože se tento stav blížil již dlouho a bylo dopředu spočítáno, že k tomu dojde, byl již v roce 1990 zahájen výzkum a vývoj protokolu IPv6. Tento protokol byl následně do roku 1996 několikrát revidován, až v roce 1996 byl cvičně implementován v experimentální síti 6bome. Největšího rozmachu tato síť dosáhla v roce 2003, kdy do ní bylo cvičně zapojeno asi 1 000 počítačů z 50 zemí světa. Funkčnost tohoto řešení tím byla ověřena a prokázána a tak se rozhodlo v roce 2004 o ukončení této testovací sítě, ke kterému v roce 2006 došlo.

Hlavními výhodami protokolu IPv6 je dostatečně velký adresní prostor, automatická konfigurace a lepší podpora mobilních zařízení. Problém z hlediska uživatele je v tom, že tyto adresy jsou na psaní již příliš složité. IPv6 vypadá například takto „ff01:0000:0000:0000:0000:0000:0000:0101“.

Protože by ale komunikace pomocí IP adres byla pro uživatele nepříjemná a složitá, byl zaveden protokol DNS[3], který umožňuje převod mezi jmény, která jsou pro uživatele lépe zapamatovatelná, a IP adresami serverů, kam se chce uživatel dostat. Díky tomuto protokolu stačí do adresního řádku internetového prohlížeče napsat pouze jméno domény, kam se chceme dostat – například „www.seznam.cz“ a prohlížeč už se sám doptá, kde se tento server nalézá (jakou má IP adresu), a pošle správně váš požadavek.

[2] Dynamic Host Configuration Protocol = server a protokol, který se používá pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu a adresu DNS serveru.

[3] Domain Name System = servery a protokol zajišťující vzájemné převody mezi doménovými jmény a IP adresami.

1.3 Anonymita

Nyní si povíme něco o anonymitě. Teď, když jsme si vysvětlili, jak vlastně připojení k internetu funguje, možná už tušíte, že anonymita na Internetu je vlastně pouze falešným pocitem obyčejného uživatele.

Je potřeba si ale uvědomit, že váš ISP[4] má zákonnou povinnost shromažďovat údaje o navázaných spojeních a na žádost pověřených orgánů jim je vydat. (§ 97, odst. 3 zákona o elektronických komunikacích). To znamená, že ať už máte přístup k internetu přes kabelovou televizi, mobilní připojení nebo lokálního poskytovatele internetu, vždy tento poskytovatel ví, kdo jste, jakým zařízením a odkud se připojujete a jaké stránky nebo protokoly používáte. Můžeme si tuto komunikaci představit jako kdybyste někomu telefonovali, ale spojení nešlo přímo a tak byste museli přes ústřednu. Ne nějakou úžasnou a moderní. Prostě přes paní sedící v recepci, která bude mít v ruce dva telefony. Ten od vás a ten, kam se chcete dovolat. No, a každý váš požadavek si tak vyslechne a pak zopakuje do druhého telefonu. Tuto paní můžeme nazvat naším ISP. Každý požadavek vyslechne a předá, kam má. Bohužel si ze zákona musí i zapsat kdo, kdy a co chtěl.

Takže to byl váš poskytovatel internetu. Ví všechno, co děláte. Ale aby toho nebylo málo, každá webová stránka ví, odkud jste na ni přišli (myšleno z jaké IP adresy a do jakého rozsahu tato IP adresa patří a tudíž, kde vlastně asi bydlíte), jaký máte internetový prohlížeč, jaký operační systém, nastavené rozlišení monitoru, jaké weby jste navštívili předtím a spoustu rozlišení, jaké weby jsem navštívil a spoustu dalších informací.

Z těchto údajů už si můžete sami vyvodit, že úplná anonymita je velmi těžko dosažitelná, vyžaduje speciální prostředky a znalosti. Myslete na to, až zase budete chtít někomu na internetu vynadat, nebo se nějak nevhodně chovat. Někoho vystopovat je také velmi náročné a většinou to nestojí za tu námahu. Vy už totiž víte, že každé připojené zařízení k internetu má svou IP adresu a tudíž se dá najít.

[4] Internet Service Provider = poskytovatel internetového připojení

1.4 Soukromí

Soukromí je další věc, kterou vlastně už na internetu nemáme. Připojovatel o nás ví vše, stránky hodně, ale zatím jsme se ještě nezmínili o jednotlivých poskytovatelích služeb. Poskytovatelé služeb také vědí víc, než by se nám líbilo. Ať už jsou to poskytovatelé e-mailů, sociální sítě, mobilní operátoři...

Pak tu máme internetové vyhledávače. Na jednu stranu nám usnadňují život a jejich schopnost pochopit, co chceme, a vrátit nám správný výsledek se stále zlepšují. Na druhou stranu i zde jeto „něco za něco“. Zlepšují se proto, že vědí, co už jste hledali. Také třeba proto, že opět znají vaši IP adresu a tak vám vracejí odkazy, které jsou poblíž vás. Co třeba vyhledávání lidí na fotografiích podle podobnosti? Co jednou na internetu, navždy na internetu.

Přísně tajné: Nekoukat!!! Pozor na nezabezpečené přenosy dat: ICQ, Skype, http, ftp, pop3, imap. Většinou existuje zabezpečená alternativa. Citlivá data je možné zašifrovat. Soubory - zaheslované archivy.

Klidně si vezmi, neubude - Elektronická data kopírováním neztrácejí. Podívejte se kdo jsem, kde všude jsem byl, co jsem tam dělal, s kým se znám a jaké jsou mé zájmy. Miluju své kamarády...Součástí základní morálky by mělo být respektování cizího soukromí.

Moderní technika umožňuje zaznamenat prakticky cokoliv a kdekoliv. Často aniž by si to zaznamenávaní lidé uvědomili. Pozor - zveřejnění takových záznamů může být protizákonné! (Zákon č. 40/1966, Občanský zákoník. §11)

2 Bezpečnost

Několik otázek: Je vůbec nutné nějak zabezpečit svoje data? Jaká data je potřeba chránit? A proti čemu je vlastně chráníme? Jaké k tomu máme prostředky? Dá se na ně spolehnout?

Vždy existuje nebezpečí zneužití. Vaše data nejsou v bezpečí, ani když je počítač vypnutý. Pokud tedy nejste experti na bezpečnost, žádná

ompromitující data raději nevytvářejte a neschraňujte. Smazané není nutně nenávratně pryč. I nečitelné se často dá přečíst.

2.1 Hesla

Nepoužívat hesla jednoduchá ani uhodnutelná (1234, heslo, love, qwert1234, křestní jméno). Nepoužívat jedno univerzální heslo. Na cizích počítačích si dát pozor na zapamatování hesla. Nepoužívat kontrolní otázky pro reset hesla. Dát si pozor, kam heslo píšeme.

Nepoužívat pochybné počítače k choulostivým operacím. Hrozí, že jsou nakaženy nějakým špehovačem. Od kompletní krádeže identity mne dělí pouze heslo do E-mailové schránky.

Zapomněli jste heslo? Nové vám přijde E-mailem. Odpovězte na kontrolní otázku.

Soukromé informace také nemusí uniknout jen vaší vinou. Poskytovatelé služeb se taky někdy utnou.

2.2 Viry, červi, koně...

Vlastní počítač se také může nakazit virem, trojským koněm nebo jinou havětí. Nepodceňovat aktualizace systému.

Používat antivir a nejlépe i firewall.

Neotvírat podezřelé soubory a opatrně pracovat s výměnnými médii.

Nelegální programy jsou spolehlivým zdrojem softwarového nebezpečí. Viry, červi a trojské koně nechtějí ničit, ale špehovat, spamovat, krást, vydírat a zneužívat.

2.3 Selhání...

Technika není spolehlivá. Internetová služba nemusí být dostupná. Úložné zařízení může selhat. Vlastní blbost nezná mezí. Kdo si omylem nikdy nic nesmazal?

Takže: zálohovat, zálohovat, zálohovat!!! Nejlépe pravidelně - zdatní mohou i automatizovat.

3 E-mail

Odesilatel uvedený v hlavičce mailu může být podvržen. Bez digitálního podpisu nelze zaručit pravost. Většinou jsou přenášeny bez jakéhokoliv šifrování.

Systém příloh není vhodný pro větší soubory. Pozor na seznamy adresátů a odpovědět všem.

3.1 Podvodné e-maily a weby

Vydávají se za legitimní služby. Odkazy vedou na podvodné stránky. Umožní pracovat - hlavně se službou, hesla ale sledují.

Většinou stačí ověřit správnou adresu. Pozor, útočník může mít adresu velmi podobnou!

Prohlížeče zobrazují stav zabezpečení komunikace.

3.2 Sdílení dat přes Internet

Menší soubory lze zabalit do archivu a poslat mailem. Problém s některými typy souborů.

Dobře lze využít datových překladišť. Ideální je mít k dispozici vlastní server. Pro fotky webové galerie, např. Picassa (opatrně na choulostivé fotografie). P2P sítě

4 Facebook

4.1 Klady

- Možnost udržení kontaktu s potenciálně velkým množstvím lidí.
- Solidní přehled o společných známých.
- Zjištění jmen lidí známých od vidění.
- Snadná cesta k seznámením s novými i předem vytipovanými lidmi (na to ale pozor...).

- Mocný komunikační nástroj pro organizaci větších akcí.
- Snadné sledování novinek týkajících se produktů, zájmových aktivit apod.

4.2 Zápory

- Pomalá odezva webu. Často nedostupné podsystémy.
- Strašná spousta aplikací pohlcujících čas a soukromé údaje.
- Užitečné informace se ztrácejí v záplavě výpisů aplikací a bezduchých komentářů.
- Možnost zneužití cizí identity.
- Nutnost brát ohled na archivaci a dostupnost komentářů.

4.3 Pozor!

Všechny okruhy vašich přátel (kamarádi z hosp... vlastně ze školy, rodiče, děti z kroužku atd.) vidí stejné informace. Fotografie přáteli okomentované vidí i přátelé přátel.

To, že soukromá data jsou dostupná pouze přátelům, ještě neznamená, že se od nich nebudou šířit dál (ať už vědomě nebo nevědomě.)

Vykrádání bytů na základě informací o dovolených nebo jiné krádeže.

Poznámky k textu