

BEZPEČNOSTNÍ MANUÁL PRO EXTRÉMNÍ PRÁCI NA iNETU

20.07.2005 - (1659 čtenářů)

MANUÁL jsem se rozhodl napsat díky rostoucí angažovanosti nacionalistů na síti a několika lidem vyznačujících se nebezpečnou činností, kterou můžeme pozorovat i na našem portálu ODPOR.NET a internetové síti vůbec. Jejich neznalost a doufejme, že nebeznadějná nedbalost, velmi napomáhá všem odpůrcům k dekonspiraci a postupné likvidaci jejich činnosti. Jedná se o příznivce, kteří jsou příliš mladí a zatím hledají zkušenosti nebo staré bijce bez dlouhodobé praxe s PC. Po prudkém sledu událostí tito lidé obvykle nejdou ke dnu sami, ale naopak s dalšími kamarády co s nimi, v naivní víře v ně, spolupracují. Celé díky lenivosti, nechuti dát trochu času, peněz nebo toho pohodlí navíc. Jak se mne vždy ptal můj kamarád a učitel. Je lepší obětovat 10 minut na cestu do internetové kavárny nebo 10 let v kriminále a připojit se z domu? Tuto alegorii si připomínám pokaždé, když na sobě pocítím dotek pracky toho Zeleného Ďábla lenosti. A? Funguje to!

PRVNÍ VĚC. Seznámení se základními fakty, které musíte před bezproblémovou prací na síti znát:

Při každé návštěvě na Internetu zanecháváte stopy. Vaše chování na síti se přesně registruje a dokumentuje. Po přihlášení svého počítače do sítě dostáváte tzv. IP-adresu (=internetová adresa protokolu, osobní poznávací internetová značka) a podle ní vás lze identifikovat (váš domácí počítač nebo třeba počítač v práci), proto je nejlepší pro vážné věci používat počítač anonymně např. v internetové kavárně. Někdy vás taky může kontrolovat správce sítě a např. v rámci podniku vám dá výstrahu: pane XY, neměl byste tak často v pracovní době vyhledávat „extremistické“ stránky. Pak většinou následuje udání. Do vašeho počítače na síti lze též při některých úkonech bez vašeho vědomí nainstalovat soubory, které (například) zaznamenávají každé klepnutí do klávesnice (keylogger). Vše co jste napsali. Texty, hesla, loginy...

Obecně se tomu říká spyware. Ten pronikne do hard-disku a registruje vaše on-lineové chování - jaké stránky a jak dlouho sledujete, co jste si stahovali atd. Prohlížeč, který používáte (např. Internet Explorer nebo Netscape Navigator) vás na to, že vám chce někdo nainstalovat cookies upozorní, ale jen v případě, že si sami tuto možnost aktivujete. Anonymně a bez toho, že by k vám pronikly soubory cookies, jde surfovat například přes stránky www.anonymizer.com, kde to pro vás udělají zdarma, jen se váš internetový čas prodlouží o 40 sekund on-line.

E-maily nejsou v žádném případě důvěrné! Přečíst si je může každý, kdo trochu rozumí počítači. Je to jako byste posílali pohled poštou. Proto stejně jako telefon nepoužívejte e-maily ke sdělování ničeho důležitého. Při psaní vzkazů nesmíte používat jména, tel. čísla, fotky, pozvánky na koncerty... a ani nic, co by kohokoliv, kdo monitoruje tuto poštu, dovedlo k vám nebo kamarádům. To by šlo jedině v případě, že máte nějakou utajenou adresu o které ví jen členové vaší buňky (dohodli jste se na ní ústně už před tím). Samozřejmě i když takovou utajenou adresu zřizujete, nesmíte to udělat doma, ale někde anonymně a tak se k ní i přihlašovat. Za pozvání své zrzavé dívky s velkými nadry ve středu večer do parku, vám těžko kdo co může. Především se nesmíte připojovat z vlastního domácího počítače ani z některého počítače třeba u vás v práci (pak se dá vždy nakonec vysledovat, že jde o vás).

Jediná možnost je připojit se z počítače v některé internetové kavárně. Kavárny ale musíte střídat a nikdy se 3x po sobě nepřipojit z jedné a téže! Pokud se, ale vždy připojujete (nebo jste nuceni se připojit) z kaváren v jednom městě (pracujeme s předpokladem velkého města jako Praha, Brno, Ostrava..) nebo určité menší oblasti, tak má policie i tak nějaké vodítko. Teď bude záležet už jen na vaší chytrosti. U neznámých lidí, se kterými přijdete do kontaktu (zájemci o členství atd.) buďte velmi obezřetní. Pokud možno si e-mailem domlouvejte jen čas a místo, kde se sejdete, abyste se domluvili ústně. Člověka si zdálky omrkněte, stejně tak ostatní kolem (lidi v autech, vchody, okna...). Na samotné místo setkání za sebe, jako vlastníka mailu, pošlete někoho jiného. Nikdy se nedomlouvejte přímo na místě srazu. Bavte se tam třeba o počasí. Místo: Nejlepší je to někde v restauraci, kde je trochu větší hluk, v hypermarketu nebo někde blízko tekoucí vody. Tím ztížíte odposlech. Možná se vám budou takové způsoby zdát jako z levné špionážní literatury, ale jde o vaši bezpečnost a být trochu paranoidní v době levné elektroniky vůbec neškodí. Prostě stále vše promýšlejte a prověřujte.

BEZPEČNOSTNÍ MINIMUM:

1. Používat PROXY

Představte si v dnešní době, že policie není zcela negramotná a sleduje speciálními odbory e-mailovou korespondenci osob, které jí mohou zajímat nebo si může vyžádat informace o tom, kde jste se pohybovali u ISP (Internet Service Provider - poskytovatel internetu). Teoreticky, jestliže někdo vytvoří www stránky, kde bude schvalovat nějaký tr. čin (např. populární útok na Strýčka Sama), může se stát, že vás policie, díky ISP, slavně vypátrá a dopadne. To samé platí pro internetové diskuze. Také přezdívané, diskuze o hovně. Můžete tomu zabránit pomocí proxy serveru. Proxy server vlastně postaví mezi Vás a stránky které prohlídíte jakousi zeď a vypadá to, že na tyto stránky přistupuje proxy server a ne vy. To se hodí zejména při návštěvách levicových prezentací a veřejných diskuzních for. Pokud se podíváte do zdrojového kódu anarchistických stránek, najdete odkaz na službu tracking IP, tedy stopování IP adresy návštěvníků.

2. Zakážete používat javu, active x, zákaz cookies

Tím zabráníte virům, trojským koním nebo jiným backdoorům, dostat se do vašeho pc. Pokud budete chtít surfovat po hambatých stránkách a nepůjdou vám obrázky nebo flashové webkamery, není nic jednoduššího než požadované funkce, v menu Možnosti sítě internetu, znovu povolit. Pokud máte ve vašem prohlížeči zapnuty Java scripty a ActiveX můžete si být jisti, že není zase tak velký problém získat IP adresu vašeho počítače a e-mailovou adresu. Od toho se dále odvíjí další děj jako získání vaší fyzické adresy, jména a telefonu. A nezáleží na tom, jestli používáte PROXY SERVER a nebo ne!

3. Čistý disk

Další problém je v tom, že i windows a internetový prohlížeč schraňují a ukládají data o tom, kde jste se na internetu pohybovali a co jste dělali. Některé tyto soubory není možno smazat normální cestou. Pojmenujte věci zkratkami, ne pravými názvy (např. Pohádky peckové babičky budou manuály C18). Veškeré věci, co jste v PC smazali přes koš, jdou zpětně obnovit (na tom už zkončilo mnoho lidí). Existují však programy, které to rádi udělají za vás. Např. WindowsWasher (<http://www.root.com>), CyberScrub (<http://www.cyberscrub.com>) a jiné (<http://www.slunecnice.cz>).

4. E-mail

Pokud vám přijde e-mail s přílohou od někoho o kom jste v životě neslyšeli, vždy zkontrolujte příponu příloženého souboru. Ta je maskovaná a označuje spouštěcí se aplikaci (např.

iloveyou.doc.exe nebo iloveyou.doc.srt). Pokud bude v pořádku, nechte ji proskenovat antivirem, což dnes většina post serveru nabízí. Obecně platí na divné přílohy ani neklikat, neotvírat, nestahovat. Existují maily, které už při otevření napadají počítač. Takové neotevírejte a hned v menu zničte. Mají většinou zvláštní adresu odesílatele a hlavičky jsou v angličtině.

5.Firewall (ohnivá zeď)

Isoluje Váš počítač od Internetu používáním "zdi kódů", které prověřují individuálně každý packet, který přichází k Vám z Internetu či odchází od Vás do Internetu, aby určily, zda jim má být průchod povolen nebo zakázán. Velmi laskavá věcička.

DRUHÁ VĚC. Zde je několik rad pro ty, co se hodně pohybují na internetu:

I. Systém o vaší počítačové aktivitě ví a sleduje vás:

Sledování nemusí probíhat klasickou filmovou metodou. Stačí vaše tušení, případně špatné svědomí. Naučte se používat instinkt, který má naše rasa zvláště vyvinutý. Oni nejsou tak hloupí, aby o sobě dali vědět. Teď jde jen o to, jak moc je zajímavé a jak dlouho si s vámi chtějí hrát. Pokud budete chytrí, časem je to přestane bavit a najdou si snadnější kořist pro ukojení svých výsledků chtivých šéfů.

1. Používejte výše zmíněné BEZPEČNOSTNÍ MINIMUM. Budou se vám snažit dostat na disk.
2. NIKDY se na "důležité věci" nepřipojujte z domu. Pokud vás sledují, tak ani PROXY nepomůže. Tedy používejte kavárny.
3. POZOR, v kavárnách kromě "důležité věci" nenavštěvujte extrémistické stránky, které na vás upozorní majitele. A stránky vztahující se k vlastní osobě (posílání SMS kamarádům, e-bankovníctví, účty, civilní mail..). To vše na vás ukáže prstem.
4. Opět i v kavárně dbejte na BEZPEČNOSTNÍ MINIMUM, jak to nejvíc jde. Admini často mají zablokované nastavení pc. Ale přesto se snažte po sobě mazat historii (menu Možnosti sítě internetu) a krátit čas na horké půdě místa činu.
5. Používejte prohlížeč Mozilla Firefox. Není tak děravá jak Explorer.
6. Vždy se rozhlédněte, jestli při cestě do kavárny není kamera, divné auto (většinou červená Felicie) a co je důležité, jestli vnitřek kavárny není natáčený. Též je dobré hlídat si lidi, co sedí kolem vás. Nutností je mít otevřeno více oken pro překrývání toho, na čem pracujete (přijde nový zákazník, někdo se dívá...). Zvědavá obsluha může vlastnit software umožňující pohled na váš monitor nebo seznam stránek, které prohlížíte. Toto vám dává více šancí.
7. Nechoďte dovnitř provokativně oblečení. Vysoké boty a kšandy těžko způsobí to, že si vás obsluha, na pozdější dotazy policie, nezapamatuje. Dobrá je neustále nasazená kšiltovka a neutrální oblečení.
8. Nepište stejným stylem (články pro web). PČR má specialisty schopné poznat vás na deseti místech najednou podle toho jak píšete (slovního vyjadřování, které používáte).
9. Nežřizujte mail u evropských internetových poskytovatelů a už vůbec ne v ČR! Podle totalitních zákonů EU je poskytovatel služby povinen odevzdat státním úřadům vaše heslo, loginy z IP adres... prostě vše. Tohle je největší idiocie. Zaručený "One way ticket to Treblika".
10. Při vytváření hesla kombinujte číslo a text. Nikdy ne údaje vztahující se k vaší osobě (jméno přítelkyně, matky...) nebo slova vám příbuzná (skinheads, internet, afa...). Pro zajímavost pirátský program wwwhack dokáže pomocí textového souboru s možnými slovy vztahujícími se k vaší osobě zadat do políčka heslo a otestovat ho až 100 jmen za minutu.

Bezpečnost zaručí neutrální slovo a číslo bez mezery. Hesla průběžně měňte a snažte se, aby jste neměli stejné i u jiných účtů.

11. Komunikujte pouze šifrovaně přes PGP (www.pgp.com). Tento systém používají banky pro bezpečnost převáděných údajů. Systém šifer nebyl dosud prolomen. Program po zadání hesla vygeneruje veřejný klíč, který předáte kamarádovi, ten předá svůj vlastní. Každý z klíčů má své id.číslo, které vzájemně ověříte nemonitorovanou cestou. Pak teprve komunikujete. Napsanou zprávu zakódujete kamarádovým veřejným klíčem (neznáte jeho heslo, nebudete ji už moci rozkódovat) a pošlete ji. On odpoví stejně.

11. Telefon NIKDY neberte s sebou. Určí vaši polohu. Tedy i místo odkud se připojujete. Lze zpětně vyžádat.

12. ICQ. Tento slavný kecálek může přinést mnoho problémů. Nejen, že je to hlavní brána virů do PC, ale nepřátelům pomůže rozkrýt síť lidí, se kterými jste v kontaktu. Řešením může být obdoba ICQ Trillian. Ten dokáže zprávy ukecaných pravičáků zašifrovat, viry přes něj rovněž nejdou. Což může být výhoda. Přesto nebezpečí rozkrýtí zůstává.

13. DC++, soukromé FTP servery s hudbou, materiály. Vybírejte pouze zahraniční poskytovatele. Pozor na IP.

14. Veškeré závadné materiály si ukládejte na náhradní HDD umístěný v plastickém boxu, které můžete rychle schovat na bezpečné místo. Pokud nepracujete s velkým objemem dat, problém řeší levná flash karta zaručující absolutní bezpečí při případné domovní prohlídce.

15. Pro paranoiky: BIS má přístroje, jimiž dokáže slyšet přes stěnu. Složit večer obraz z odrazu blikání a frekvence monitoru na sklo vašeho okna. Pokud je hodně zajímáte a potřebují vás dostat. Počkají, až půjdete do práce, vlezou vám do bytu a zasádnou do zdi miniaturní kameru s otvorem pro snímání jako dvě špendlíkové hlavičky, co snímají monitor. Případně štěnici nebo maskovaný spyware do pc. Takové hračky dnes přijdou na mizerné dva a půl tisíce. Což je pro ně směšné. Tuto věc lze zjistit (alespoň dřív) přeježděním mobilu po zdi. Tam kde je štěnice vám opakovaně ubudou čárky signálu, nebo zakoupením detektoru, rušičky. V PC to jde kombinací kláves CTRL+ALT+DELETE a v oblasti Procesy zrušit, odstranit podezřelý proces.

II. systém o vaší počítačové aktivitě neví:

Což ale neznamená, že se v budoucnu nedostanete na černou listinu. A jak už víme, vše lze vyvolat zpětně.

1. Dodržujte alespoň polovinu triků, které jste se naučili v předchozím oddíle.

2. Praktikujte BEZPEČNOSTNÍ MINIMUM.

3. Návštěva X-chatu je kapitola sama o sobě. Dobré místo na sbalení baby, špatné na propagaci čehokoli. Toto komunikační médium je nepřetržitě sledováno speciálními programy a policií už několik let. Programy vyhledávají klíčová slova, která napíšete (Národní Odpor, rahowa, zbraně, lolita...) zobrazené výsledky okamžitě kontrolují stálí správci a předávají je policii. Opět známý postup. Zachycení IP adresy, předání výkonným orgánům, návštěva. Proto buďte opatrní, nikdy nevíte, jestli "kamarád na chatu" není náhodou nějaký zrasnej fízl!

4. Snažte se utajit činnost a možnost získání vstupenky na černou listinu orgánů PČR.

Jednoduše řečeno: stále namáhejte nejen své svaly, ale hlavně svůj mozek. Buďte nedůvěřiví a opatrní, tím nic nezkazíte.

Tak a máte to za sebou. Doufám, že to bylo náročně a leccos nového jste se dozvěděli. Na téma bezpečnost se dá psát stále. Bylo by dobré udělat ještě několik publikací. Namátkou na mobilní telefony, pohyb na ulici, ozbrojené střety s levicí. Pokud máte chuť přiložit ruku k dílu, posílejte své práce na redakce@odpor.net. Budeme vděční za každou pomoc kamarádi. Co závěrem? Vybral jsem slova hlavního zpěváka kapely Fortress, Scotta. "V současné době musíme vést boj především přes moderní technologie. Mají ohromné propagační možnosti jako nic před tím. Těch je nutné plně využít. Musíme v nich být neustále o krok před nimi. Protože naše vůle učit se je silnější než ta jejich. A to nás předurčuje k vítězství."

Autor/Zdroj: Ing. Jirka Ponorka