Největší rizika na internetu

Jaká nebezpečí a nástrahy na nás čekají a jak se jim ubránit (CD)

VOJTĚCH BEDNÁŘ

Že internet je džungle, v níž každému, kdo se tam ocitne hrozí spousta různých nástrah a nebezpečí, ví dnes každé malé dítě. Jaká rizika to ale jsou? Jak konkrétně nás (a nejen naše počítače) ohrožují? A jak se jim můžeme bránit? To vše se dozvíte právě zde.

Bylo nebylo, na počátcích současného on-line věku existovalo několik, vzájemně nepropojených počítačových sítí. Patřily velkým korporacím, ale některé byly také zcela otevřené a amatérské. Zejména ve Spojených státech byla na počátku devadesátých let přítomna síť America Online, v menší míře, po roce 1995 také The Microsoft Network, čili MSN. Všechno, co dnes známe jako služby, byly vlastně samostatné, více či méně mezi sebou komunikující a především placené sítě. Tyto sítě byly tvořeny po softwarové stránce zcela homogenním prostředím. Mnohé z toho, co je drželo pohromadě dodnes existuje, avšak již v pozměněné podobě, v podobě k nepoznání. Jako například software AOL, portál MSN a další.

Tyto homogenní sítě vynikaly jedním podstatným kouzlem. Relativní bezpečností. Protože jejich software byl jednoduchý, obsahoval jen málo míst, která by se dala využít k zlovolným účelům. Samozřejmě existovala možnost šíření virových nákaz prostřednictvím elektronické pošty, avšak ta nebyla zdaleka tak hojně využívána jako dnes, a především také škodlivé kódy, které by se jí mohly šířit, byly značně primitivního rázu.

S integrací všech těchto sítí do jediného monolitu – internetu, se otevřela brána, přesněji řečeno mnoho různých bran těm nejroztodivnějším způsobům, ohrožujícím samotné části nově vzniklé sítě. Tedy počítače, síťové prvky, software a dokonce, zprostředkovaně, uživatele. Gigantický organismus internetu se skládá z mnoha propojených částí, přičemž je můžeme velmi snadno rozdělit na vnitřní a vnější. Vnitřní části jsou páteřní spoje, rozvody, přepínače, směrovače a servery všeho druhu. Vnější část internetu pak představují uživatelské prvky – osobní počítače, ale čím dál tím častěji i jiná, například přenosná zařízení.

Vnitřní část internetu, podle předchozí definice, je poměrně heterogenní. Různé prvky mají různou elektronickou stavbu, někdy podle svého určení, jindy podle výrobce. Využívají různé operační systémy, dokonce různě složité systémy, od jednoduchých implementací uložených často v jediném ROM čipu až po komplikované UNIXy. Komunikují spolu v různě složitých protokolech a díky univerzálnosti těchto protokolů, tedy ne jednotlivých zařízení, jsou schopny si navzájem porozumět.

Naproti tomu vnější svět, tedy planeta uživatelských stanic, je poměrně jednobarevný. I když teoreticky existují taktéž různá zařízení od různých výrobců obsahující různé systémy a komunikace probíhá převážně na bázi protokolů, skutečnost je poněkud odlišná. Desktopový svět je fakticky jednobarevný. Je postaven na operačních systémech typu Microsoft Windows a jejich vlastní implementaci protokolů a dalších standardů. I konkurenční systémy, opěvovaný Linux a jeho varianty a další, prakticky jen kopírují mnoho principů, které mají svůj původ v majoritním systému. V důsledku toho s sebou nesou mnoho jeho nedostatků, čímž přispívají ke skutečnosti, že vnější sféra internetu je homogenní možná až příliš.

Teorém zlého člověka

Za každým technickým rizikem stojí zlý člověk. Kdyby nebylo lidí se zlými úmysly, nebylo by třeba žádného zabezpečení ničeho před ničím. Jestliže elektronická komunikace je v současné době oborem lidské činnosti, kde se zabezpečení rozvíjí nejvíce, můžeme čekat, že právě zde je nejvíce zlých lidí? To samozřejmě ne, ale elektronická komunikace, zvláště internet má velmi mnoho zvláštností, které tyto lidi přitahují, a navíc nekalé úmysly probouzejí i v těch, u nichž bychom je nikdy nehledali. Činnost jedince, která by v reálném prostředí byla destruktivní jen v minimální míře anebo spíše vůbec, může mít na internetu velice snadno nedozírné následky, je-li úspěšná. Všechny technické prostředky, vynaložené na zabezpečení virtuálního prostředí, jsou na tuto činnost vynakládány právě proto, aby se zabránilo konání těchto „zlých lidí“, i když i sám tento pojem je zavádějící.

Rizika kam se podíváš

Jestliže je internet technickým, velmi složitým organismem tvořeným propojenými elektronickými zařízeními s různým softwarem, v některých mís-

tech homogenním, jinde nikoliv, a jestliže jsou jeho podstatou informace, které tento hardware a software přenášejí, pak jsme vlastně definovali podstatu rizik, jež souvisejí s používáním takovéhoto systému. Největším rizikem zde je jednak nebezpečí, že informace, které jsou určeny pro přenos z bodu A do bodu B, ke svému cíli nedorazí, nebo budou nějak poškozeny či uměle zkresleny. Druhým rizikem je, že stejná informace bude během své cesty, nebo třeba při skladování na záznamovém nosiči odposlechnuta někým (C), kdo není oprávněn ji přijmout a kdo může nějakým způsobem poškodit jejího právoplatného majitele tím, že se ji dozví. Díky nehmotné povaze informací, kdy pojem krádež neznamená totéž jako odcizení – protože tam, kde lze beze ztráty jakoukoliv informaci okopírovat, o ničem takovém nelze hovořit – se navíc otázka jejich bezpečnosti ještě více komplikuje.

Dalším, specifickým problémem je riziko poškození technického zařízení, které slouží k ukládání informací, jejich zpracování a transportu, a to buďto fyzické (kopnu do toho), nebo konsekventní, způsobené špatnou funkcí instalovaného softwaru (vymažu si pevný disk). V tom případě není primárně narušována uložená (důležitá) informace, ale jednak její nosič, jednak informace, které jsou uloženy spolu s ní. Jakýkoliv počítačový program nebo protokol totiž sám o sobě rovněž není ničím jiným než informací.

Informace na síti jsou sice nehmotné, avšak mají svou, naprosto hmotnou, cenu. Lze je vyjádřit váhou jak hmotných prostředků, tak i peněz. Víme, kolik stojí operační systém, program, na kolik vyjde film na DVD, počítačová hra. To jsou pochopitelně pouze nejtriviálnější příklady, po síti se pohybují také informace nedozírné hodnoty, nejen pouze zábava jako jsou filmy nebo počítačové hry. Právě kontrast mezi jejich nehmotnou povahou, ale hmotnou cenou společně se všemi faktory, o kterých jste si mohli přečíst už dříve, tj.

- s obtížně definovatelnou homogenitou/heterogenitou internetu
- s univerzálními komunikačními protokoly
- s otevřeností a relativní anonymitou
- s přítomností „zlých lidí“

dává dohromady kaši, z níž se rodí bezpečností rizika a bezpečností útoky, o nichž bude řeč v následující části tohoto článku. Rizika, která jsou v každém případě velice reálná a na která je třeba ukázat, spíše než před nimi strkat hlavu do písku po pštrosím způsobu.

Dalo by se říci, že rizik ohrožujících jak data, která se dají finančně vyjádřit, tak i přímo uživatele, je na současné síti více než dost. Jsou zaměřena proti nejrůznějším druhům informací od naprosto specifických, jako jsou peněžní toky (to nás jako uživatele ale nemusí zajímat) po o něco obecnější, jako osobní data lidí pracujících se sítí kvůli distribuci reklamy. Poškozování informací je pak v největší míře zaměřeno jednak proti prvkům tvořícím funkční, především softwarovou infrastrukturu sítě, jednak proti vyšším (vnitřním) ovládacím prvkům této sítě, jež jí umožňují hladký běh. Lapidárně vyjádřeno, buď někomu odcizím či vymažu obsah počítače, nebo ho zasypu tolika požadavky na komunikaci, až komunikovat docela přestane. Když nemůžu ani jedno, prostě jen o něm zjistím co nejvíce informací, a poté se je pokusím nějak využít ve svůj prospěch (zkompromituji uživatele, nebo mu budu na základě zjištěných dat servírovat reklamu, ať se poměje). Všemi výše uvedenými způsoby jej nějak ohrožuji, nějak zasahuji do jeho normálního fungování, představuji pro něj jako „zlý člověk“ riziko. Kterému, jak je logické, se bude nějak bránit.

Protože žádný útočník, není-li jeho zájem omezen na jednoho konkrétního uživatele nebo jeden konkrétní síťový prvek, nemůže být všude najednou, vytvářejí si tito útočníci své vlastní pomocníky. Takzvané škodlivé kódy nejsou nic jiného než produkt „zlých lidí“, jejich prodloužené ruce, které jsou schopny v mnoha kopiích zároveň dělat to, co by jeden útočník mohl dělat jen ve velmi omezené míře nebo vůbec ne. Navíc, takhle své činnosti nemusí být vůbec přítomen, je ještě o něco lépe maskován, anonymizován za ohromnou horou samoreplikujících se kódů, kterou vytvořil.

Právě díky těmto faktorům a díky něčemu, co bychom s trochou zjednodušení mohli nazvat odosobněním internetu, je dnes síť místem považovaným všeobecně, a nutno dodat že právem, za nebezpečné. Kromě lidského hlediska samozřejmě existuje i další – technické. Současné systémy, především softwarové, jsou velmi složité a koncipované jako univerzální. Díky této univerzálnosti a pokračující provázanosti protokolů je není možné jednoduše interpretovat, a protože je nelze jednoduše interpretovat, stávají se nebezpečnými. V žádném okamžiku totiž nelze spolehlivě říct, jak se která část tohoto kódu, tohoto komplikovaného systému bude chovat. To otevírá lidem se zlými úmysly, přesněji řečeno jimi vytvořeným škodlivým kódům, prakticky neomezené pole působnosti.

V minulosti bylo vytvořeno několik pojmů, jež se dnes staly velmi oblíbenými. Patří mezi ně například bezpečnostní mezera (o nich si povíme dále). Přestože jde o věc, která je svou podstatou naprosto chimérická, reálně neexistuje a představuje prakticky jen jakousi možnost, možný postup v miliardách dalších možných variant, je jí věnována zvláštní pozornost. Zvláštní přitom je, že některé projevy chování informačních systémů, které jinak naplňují všechny znaky společné bezpečnostním mezerám, za tyto mezery považovány nejsou. Velmi podobné to je s některými škodlivými kódy, ale také specifickým chováním uživatelů, fyzických lidí pracujících se sítí. To je ovšem otázka poněkud jiné logiky.

Základní rizika současného internetu

Posadíme se, jako uživatel, ke svému počítači připojenému do sítě. Jak jsme si na začátku řekli, a v teoretickém úvodu poněkud upřesnili, v tom okamžiku nám neustále hrozí mnoho rizik pocházejících z vnějšku sítě. Tato rizika ohrožují:

- náš počítač, jeho operační systém, aplikace
- naše data, dokumenty, účetnictví, dopisy, tabulky, všechno co jsme vytvořili a v počítači máme
- naše soukromí, osobní informace, které jsou v počítači uloženy
- naše peníze (pokud k nim z počítače přistupujeme)
- naše dobré jméno (nikomu se nelíbí, aby se jeho jménem rozesílala pornografie)
- náš čas (pokud musím dělat něco, co nesouvisí s tím, co jsem chtěl, abych se k tomu, co jsem chtěl, vůbec mohl dostat, je to jistý druh sabotáže)

To byl samozřejmě pouze značně nekompletní výpis těch nejzjevnějších rizik. Existuje mnoho dalších, jež se schovají za některá z těchto, výše uvedených, nebo která vznikají z jejich různé kombinace, jejich různé přítomnosti a různého využití. Každé z rizik se může projevit v mnoha různých, navzájem často nespojitých formách, různými projevy, ale všechna jsou nám relativně nebezpečná. Přesněji, našim datům, našim penězům, našemu času.

Červy kam se podíváš

S nástupem moderního internetu se ukázalo, že největší riziko konce osmdesátých a první poloviny devadesátých let dvacátého století – počítačové viry, na něm nemá tolik místa, kolik by se dalo čekat. Jejich místo na výsluní škodlivých kódů velmi rychle převzala jiná varianta – červy. Červ je program využívající operačního systému, přesněji řečeno jeho vyšších funkcí, stejně tak jako vyšších funkcí aplikací, především schopnosti obsahovat svůj vlastní programovací jazyk – makro, společně s nedostatkem plynoucím ze vzájemného provázání takových komponent. Základní filozofií červa je získat určitý stupeň kontroly nad strojem, do kterého se červ dostane, dále se prostřednictvím sítě rozmnožovat a vykonávat nějakou činnost. Zatímco v případě virů byla zničující – poškozující činnost směrována primárně proti napadenému počítači, u červů je tomu jinak. Mohou sice úspěšně vykrádat data ze stroje, na nějž se dostaly, nicméně to není jediné. Stejně tak dokáží i zneužít napadený stroj k útoku proti jinému, prakticky si jej zotročit. Příkladem toho může být slavný červ LoveSan/MSBlast, jenž byl primárně určen k vyvolání útoku na operační systém serverů jedné konkrétní společnosti.

Nedostatky systémů, které červy zneužívají, jsou jen málokdy tak zjevné, aby je bylo možné použít bez přímé interakce s uživatelem. Prakticky to znamená, že ten kdo sedí u počítače musí často červa především nějak „pustit dovnitř". To se děje nejčatěji otevřením přílohy nakaženého e-mailu, a tím spuštěním kódu, který se v této příloze nachází. Jinými slovy, tak je červ usazen do operačního systému, velmi často s využitím nějakého jeho nedostatku. Červy často využívají dokola stále stejných nedostatků, a uživatelé naprosto mechanicky stále dokola opakují téže chyby – pouštějí je dovnitř.

Jinou formu představují červy, jež nevyžadují přímou interakci s uživatelem, nejsou přílohou e-mailu, ale ke svému šíření využívají objevený, zjevný nedostatek systému. Příkladem tohoto může být opět náš známý MSBlast, který se šířil napadáním jedné části Windows NT. Díky homogennímu prostředí vnější části internetu, o němž už byla řeč, může takový červ s poměrně velkou jistotou sázet na to, že ve svém okolí najde dostatečný počet počítačů, které může ke své činnosti využít.

Obrana proti červům působícím v rámci e-mailu je jednoduchá – neotevírat podezřelé přílohy. Která příloha je podezřelá a která nikoliv, nelze přesně vyjádřit, ale lze to velmi snadno intuitivně odvodit a nebezpečný e-mail rozpoznat. Ve druhém případě je problém složitější. Homogenita operačního prostředí přináší kromě rizika existence živného prostoru škodlivým kódům (jako v každé monokultuře) také výhodu. Objevené mezery, nedostatky, které mohou červy využít pro své šíření, lze také poměrně rychle řešit. Programátoři operačních systémů v současnosti také pracují na hledání a odstraňování takovýchto bezpečnostních mezer pomalu více, než na vývoji vlastních systémů. To je ovšem daň za jejich složitost.

Je zodpovědností každého uživatele, aby se proti červům bránil na dvou frontách zároveň. Především kvalitním antivirovým/antičervovým prostředkem. Antivirový systém by měl být součástí každého počítače, zejména pokud je trvale, nebo i jen dočasně připojený k internetu. Současné antivirové systémy poskytují poměrně rychlou a solidní ochranu před aktuálními hrozbami, stejně tak jako jejich likvidaci v případě, že se takovýmto červovým hrozbám již podaří systém napadnout. Mezi nejznámější antiviry, které lze použít v domácím prostředí, patří:

- **Avast Antivirus** (*www.avast.cz*)
- **AVG** (*www.avg.cz*)
- **Nod32** (*www.nod32.cz*)
- **Norton Antivirus** (*www.symantec.cz*)
- **Kaspersky Antivirus** (*www.kaspersky.cz*)

Vždy je třeba mít na paměti, že i když nějaký antivirus v počítači mít musíme, může to být pouze **jeden** z nich. Kvalita antivirů je různá, stejně tak jako jejich cena *(www.viry.cz)*, vždy platí že ten, který používáme, by měl být pravidelně aktualizován.

Antivirové aplikace řeší červy, ale ne bezpečnostní mezery. Každý operační systém připojený k internetu by měl být stejně jako antivirus udržován v aktuálním stavu, tj. s maximem možných bezpečnostních záplat – řešení slabých míst. U systémů Microsoftu je univerzálním výchozím bodem pro získání a automatickou instalaci těchto záplat systém Windows Update *(www.windowsupdate.com)*. Tento systém dokáže snadno detekovat slabá místa počítače a následně je řešit – tedy instalovat opravy, pokud existují. Moderní operační systémy jsou také vybaveny možností automatické aktualizace, kterou je navýsost dobré nechávat v zapnutém stavu stůj co stůj.

Pokud chceme mít alespoň základní přehled o stavu svého systému, tedy o tom nakolik je bezpečný, je čas od času dobré využít některý z bezpečnostních analyzátorů. Základním z nich je MBSA (Microsoft Baseline Security Analyser), který je zadarmo ke stažení z internetu (bližší informace o něm najdete např. na *www.zive.cz/h/Viryabezpecnost/Ar.asp?ARI=115048&CAI*. Jinou variantou je on-line analyzátor společnosti Symantec, dostupný na jejím webu *(www.symantec.cz)*.

Jak si zachovat bezpečnost a soukromí

- Aktualizovaný operační systém
- Aktivní a aktuální antivirový program
- Aktivní a aktuální firewall
- Antispywarová aplikace, pravidelné kontroly počítače
- Používat jen důvěryhodné aplikace
- Neotevírat podezřelé přílohy e-mailů
- Nemyslet si, že „mě se žádný útok netýká". Týká.

Útok!

Nedostatku operačního systému nemusí využívat pouze červ, ale také jedinec, zlý člověk, který nám chce nějakým způsobem ovlivnit počítač, tedy všeobecně známý hacker. I ten k tomu používá speciální software, ale jeho útok se od útoku červa odlišuje. Zatímco červu je jedno, do jakého systému se dostal, hacker se koncentruje obvykle na jediný, konkrétní. K tomu musí přesně znát jeho nedostatky a možnosti. Obecnou obranou proti hackerů, ale také dalším rizikům, je použití firewallu. Existuje několik typů firewallu podle jejich funkce a umístění. Patří mezi ně hardwarové firewally, fungující jako brány do internetu pro skupiny počítačů, softwarové, integrované do operačních systémů a softwarové dodatečné, takzvané osobní. Existují přibližně tři firewally, se kterými se můžeme setkávat nejčastěji na uživatelské straně. Patří mezi ně:

- **Zone Alarm od společnosti ZoneLabs** (*www.zonealarm.com*)
- **Kerio Personal Firewall – Kerio** (*www.kerio.cz*)
- **Firewall, který je součástí Norton Internet Security** (*www.symantec.cz*)

Stejně jako v případě antivirové aplikace, můžeme mít na jednom počítači pouze jeden firewall. To, co ale vůbec nevadí, je kombinace osobního firewallu na počítači s firewallem v podobě internetové brány u našeho poskytovatele připojení – relativní bezpečnost se tak jen zvýší. Firewally představují elementární ochranu proti hackerům, i když tato ochrana není stoprocentní. Jsou schopny maskovat a blokovat určité porty protokolu TCP/IP, monitorovat připojující se aplikace, reagovat na jejich změnu a také na jejich nekorektní chování, pokusy stát se serverem a podobně. Umí rovněž zachytit pokusy o vzdálené převzetí kontroly nad počítačem, záměrné zavlečení škodlivého kódu a další činnosti, které mohou být projevem probíhajícího bezpečnostního útoku. Vždy je nejen dobré, ale přímo nutné kombinovat je s fungujícím a aktuálním antivirovým programem a aktuálním operačním systémem.

Útěk informací

Spyware, tedy takové programy, které aniž by se rozmnožovaly jsou schopny z různých důvodů sledovat činnost počítače a uživatele, již dávno nejsou něčím novým, přesto je jejich působení často podceňováno. Pokud by šlo pouze o aplikace, jež sledují naše navštívené stránky, aby nám mohly nabízet relevantní reklamu, nebyl by problém tak veliký. Potíž ale spočívá v tom, že tyto softwarové prvky jsou schopny z napadeného systému také aktivně vykrádat data, třeba použitá přihlašovací jména nebo hesla, údaje o používání různých aplikací a podobně. Vzhledem k tomu, že na ně standardní antivirové prostředky obvykle nereagují, jsou poměrně nebezpečné a jejich rizika nejsou doceňována. Přesto je zbavení se jich nejen prospěšné, ale navíc může podstatným způsobem odlehčit počítači – zabírají často jeho systémové prostředky, parazitují na výkonu procesoru, paměti a také na propustnosti internetového připojení. Pro odstraňování spywaru se používá několik aplikací, avšak v našem prostředí se nejvíce ujaly dvě:

- **Lavasoft Ad-Aware** (*www.lavasoft.de*)
- **Spybot Search & Destroy** (*security.kolla.de*)

Obě aplikace vycházejí, co se kvality týče, zhruba nastejno. Spybot je určen spíše zkušenějším uživatelům a je schopen detekovat větší rozsah hrozeb. Ad-Aware je naproti tomu komerčním produktem, byť existuje verze, která je pro domácí použití k dispozici zadarmo. Dá se říct, že první z programů je schopen hledat škodlivý software rychleji, druhý sofistikovaněji. Jejich kombinace se stejně jako v předchozím případě nedoporučuje, i když nezpůsobuje problémy takového rozsahu, jako kombinace antivirů. Podrobnější informace o tom, jak se spywarem bojovat, se dočtete v článku autorů Davida Čepičky a Daniela Behrense „10 tipů proti spywaru".

Hygiena především

Internet není bezpečným místem, je na uživatelích, aby se před většinou rizik obrnili a přitom neztratili schopnost jej kvalitně a bez obav používat. Zásady informační hygieny, tedy používání dříve vyjmenovaných prostředků a především takové schování, které nám ani našim informacím, stejně tak jako jiným uživatelům, neublíží, je krokem k úspěchu a to je třeba mít na paměti. 4 0261/FEL ❑