Bezpečnost na Internetu

Luděk Matyska, ÚVT a FI MU

Bezpečnost Internetu a bezpečnost práce na Internetu se stává stále více sledovanou oblastí počítačových sítí a návazných programových systémů, včetně aplikací. S růstem naší závislosti na Síti rostou požadavky na její spolehlivost a bezpečnost, přitom v mnoha případech nelze tyto dva pojmy striktně oddělit: Potřebujeme-li přístup ke konkrétním datům na konkrétním serveru, pak je nám v podstatě lhostejné, zda nedostupnost je způsobena výpadkem hardware nebo třeba operačního systému (což řadíme do oblasti spolehlivosti) nebo zda je to důsledek napadení viry či DoS útoku (Denial of Service, tedy znepřístupnění služby) a patří tedy do oblasti bezpečnosti. Obdobně, začne-li server rozesílat číslo naší kreditní karty, které jsme mu svěřili jakou součást obchodní transakce, nezáleží nám příliš na tom, zda je to důsledek záludné chyby v programu, neodhalené v průběhu testování, nebo výsledek útoku. Našim přáním je mít jistotu, že veškerá data, která Internetu svěříme, se dostanou pouze těm, kterým jsou určena, a že všechny transakce, které provedeme, provádíme vždy vůči těm, které na druhé straně očekáváme. Z pohledu uživatelů je tedy žádoucí homogenní prostředí s jasně definovanou úrovní spolehlivosti a zabezpečení, případně několik takových prostředí, jiné pro nezávazné „surfování“ po Internetu a jiné např. pro komunikaci s naší bankou.

Všichni dobře víme, že síla řetězu je dána silou jeho nejslabšího článku. Obdobným způsobem je nutno nahlížet na Internet a jeho schopnost bránit se náhodným i záměrným chybám. Napadení počítače či skupiny počítačů je prakticky vždycky důsledek nějaké chyby: buď programové nebo lidské[1]. Cílem těch, kteří se snaží síť napadnout, je identifikace a následné využití právě těch nejslabších článků. Cílem nás ostatních je pak posílení právě těchto článků, a tím posílení celého Internetu.

Na jedné straně „pevnosti řetězu“ stojí páteř Internetu, tvořená spojovacími linkami a aktivními prvky (především směrovači), s vysokou mírou redundance, odolnosti proti poruchám a podobnými robustními vlastnostmi. Páteř je pod trvalým dohledem a je spravována kvalifikovanými odborníky, kteří jsou schopni velmi rychle zareagovat na každou nestandardní situaci. Na druhé straně oné „pevnosti řetězu“ pak stojí koncové prvky sítě, tvořené servery a především vlastními uživatelskými stanicemi. Kvalifikační úroveň se zde velmi liší, což výrazně ovlivňuje rychlost a adekvátnost případné reakce. I Internet sám je vysoce heterogenní – ostatně název říká, že se jedná o Síť sítí – a liší se i kvalita zabezpečení jednotlivých sítí.

1 Ohrožení

Největší ohrožení spolehlivosti i bezpečnosti Internetu spočívá v jeho dostupnosti a rozšíření a dále v prakticky nulové ceně přenosu informací po již vytvořené infrastruktuře. Rozšíření s sebou nese anonymitu – jistý druh kriminální činnosti je snáze realizovatelný ve velkoměstě, kde je jedinec anonymní, než na vesnici, kde se všichni znají. Určitá anonymita je sice pozitivní vlastností Internetu a je proto v centru pozornosti skupin zasazujících se za ochranu soukromí, na druhé straně je však i velmi výhodným prostředím pro nežádoucí až nelegální činnosti[2]. Anonymita s sebou bohužel často nese i pocit jisté beztrestnosti: když nevíte kdo jsem, nemůžete mne chytit a potrestat. Zatímco v reálném světě je otevírání zásuvek, případně zkoušení klíčů do cizích dveří aktivita s vysokým stupněm nebezpečí pro pachatele – bude-li přistižen, jeho

[1] Z jistého abstraktního pohledu je všechno důsledek lidské chyby: od chyby uživatele, přes chybu programátora, až po lidské selhání těch, kteří zlomyslný či dokonce zákeřný kód implementovali a vypustili na Síť. Tento pohled nám ale příliš nepomůže, chceme-li najít způsob, jak se bránit.

[2] Ostatně na tento problém narazili např. operátoři mobilních telefonů, kde předplacené karty jsou naprosto anonymní a takovéto telefony jsou ideálním doplňkovým nástrojem kriminální činnosti – policie neví, které telefony odposlouchávat a i když se nějaký hovor odposlechnout podaří, není obecně možné přiřadit konkrétní telefon konkrétní osobě bez dalších dodatečných důkazů. Nepřekvapí asi proto zákonodárná iniciativa některých států USA pro omezení prodeje a dostupnosti předplacených karet.

identita je nezpochybnitelná – v anonymním virtuálním světě tomu tak není – i když bude pachatel přistižen, je „chycena“ pouze jeho elektronická identita, kterou nemusí být jednoduché ztotožnit s identitou v reálném světě. Další výzvu představuje fakt, že v tomto případě činnost nemusí vykonávat přímo uživatel, ale může použít *avatara* – elektronického prostředníka, který ono zkoušení klik a zámků provádí za něj a pouze v případě úspěchu použije elektronický ekvivalent mrtvé schránky (dobře známé ze špionážních románů), kam zašle informace o otevřených zásuvkách či dveřích. Případně se spokojí s tím, že cílový systém nějakým způsobem „označí“, bez přímé zpětné vazby – v případě skutečně velkého úspěchu předpokládá, že výsledek je oznámen prostřednictvím médií[3].

Na jedné straně zde tedy máme snadnost, s jakou se lze v podstatě anonymně pohybovat po Internetu, doplněnou tím, že geografická vzdálenost nehraje žádnou roli. Na straně druhé pak fakt, že v Internetu je zapojeno obrovské množství zařízení, která jsou v mnoha směrech identická: je zde tedy velká pravděpodobnost, že klíč pasující do jednoho zámku bude použitelný i v mnoha zámcích jiných. Udržet takové prostředí bezpečné a spolehlivé se zdá skoro nad lidské síly. Konkrétní počítač, připojený do Internetu, je tak vlastně vystaven možnému útoku z velkého virtuálního neznáma[4].

Růst bezpečnostních incidentů má i svou technologickou podstatu, která spočívá v rostoucím počtu kopií de facto identického programového vybavení počítačů (ale i aktivních prvků sítě). Největší množství problémů mají uživatelé operačních systémů firmy Microsoft – to není jen důsledkem kvality práce při vlastním vývoji, kdy se původně vyvíjel operační systém pro nepřipojené počítače, ale zejména důsledek toho, že tyto operační systémy mají nejvíce uživatelů a tito uživatelé patří mezi nejméně poučené. Skulina, kterou se podaří objevit (tedy způsob, jak se dostat k počítači a datům na něm uloženým), je okamžitě využitelná na statisících systémů, jejichž uživatelé navíc často ani netuší, že jejich počítač zneužívá někdo další (natož aby věděli, jak příslušnou skulinu uzavřít). Podobné skuliny až díry existují i v ostatních operačních systémech, ty ale zdaleka nejsou tak rozšířené a jejich uživatelé zatím většinou patří mezi informovanější – jednak rychleji rozeznají podezřelé aktivity, jednak vědí, jak se s nimi vypořádat.

2 Ochrana – firewally?

Nejjednodušší cestou, jak se nebezpečí vyhnout, je odpojit počítač od Internetu. A ještě vyššího zabezpečení dosáhneme, pokud počítač úplně vypneme. To je jediná skutečně spolehlivá cesta, jak zabránit útokům a dosáhnout 100 % spolehlivosti (počítač bude spolehlivě vypnut). Samotné odpojení od Internetu obecně nestačí – pokud si jakoukoliv cestou (přes výměnná média) budete vyměňovat data, může být počítač napaden i takto. Drastické řešení úplným vypnutím však není skutečným řešením: počítač chceme používat, což znamená, že musí na sebe vzít i riziko výměny dat a případně i riziko, plynoucí z připojení na Internet (např. zabezpečené sítě armády nejsou vůbec propojeny s Internetem a data se musí předávat jinou cestou).

Řekli jsme výše, že Internet je Síť sítí, poměrně často se proto setkáváme s představou, že zabezpečení počítačů můžeme nejlépe zrealizovat shlukem našich počítačů do konkrétní podsítě, kterou od Internetu oddělíme speciální bránou, která bude kontrolovat procházející data a nepustí k nám (případně ani od nás) nic, co nebude schváleno. Na tomto principu pracují *firewally* – „ohnivé zdi“, obecně modifikující procházející data s cílem minimalizovat neautorizovanou výměnu informací. Tento přístup, přestože je velmi oblíben zejména mezi správci počítačových sítí, má však celou řadu spíše negativních důsledků:

– V konečném důsledku může být prohlížen každý přenesený byte, tj. z určitého pohledu se vlastně jedná o cenzuru. Přestože po právní stránce je vše v pořádku, již samotné vědomí

[3] Stejně tak je možno otevření dveří zaslat na vhodnou elektronickou nástěnku, kterou čtou statisíce lidí. Mezi nimi najít toho, jemuž je zpráva určena, je samozřejmě nemožné.

[4] Udává se, že v mnoha sítích v USA se doba od připojení nového počítače na Internet do příchodu prvního „návštěvníka“ pohybuje v desítkách minut. V ČR je tato doba podstatně delší, ale můžete celkem spolehlivě počítat s tím, že do cca 5 hodin je i Váš počítač „objeven“ a „oťukán“.

této permanentní kontroly nemusí být příjemné a motivující.

– Prohlížení dat samozřejmě není zadarmo a vyžaduje určité zdroje. Pokud stojí firewall za ISDN linkou, pak samozřejmě zpoždění vlastního datové připojení je mnohonásobně vyšší než to, které vnese do toku dat firewall. Pokud ale začneme uvažovat o skutečně vysokorychlostním připojení (gigabity za sekundu), firewall může způsobit významné zvýšení latence a snížení pozorované propustnosti.
– Firewall, to především znamená zeď a každá zeď má dvě strany. Z pohledu nových aplikací a možností není vždy jednoznačně rozhodnutelné, která z těch stran představuje lepší svět. Počítače za firewallem jsou v jakémsi *ghetu*, dovnitř a ven mohou jen „schválené“ myšlenky. Využití nové služby může přinejmenším znamenat dlouhou diskusi se správci firewallu a bohužel často končí tím, že příslušná služba (dostupná na „nebezpečném“ Internetu) není povolena – ne pro ni samotnou, ale protože by se ve zdi objevila nová „okna“, tedy místa, jimiž může přiletět dovnitř další šíp. Firewall tak můžeme v abstraktním smyslu chápat jako snahu oddělit nás od příliš dravého světa „venku“. Z historie víme, že taková snaha často končí intelektuální impotencí.
– Vytvoření interního gheta má však další velmi vážný důsledek: vytváří pocit *falešného bezpečí*. Mám-li kolem sebe zeď, velmi snadno propadnu pocitu, že uvnitř té zdi mi nemůže nic hrozit. Nemluvím teď o tom, že nemalá část útoků je zahájena zevnitř, ale největší nebezpečí je zánik imunizace pro případ proražení té zdi. Každou zeď lze buď prorazit nebo obejít, a pokud nejsem permanentně připraven, může být taková situace fatální[5]. Pocit falešného bezpečí za firewallem brání vzniku nezbytných návyků a víceméně automatických ochranných mechanismů, jejichž přítomnost je zcela nezbytná pro rychlou lokalizaci napadení a minimalizaci jeho následků.

Firewally mají samozřejmě i své pozitivní rysy, z nichž asi nejdůležitějším je stažení veškerého provozu do jednoho místa. To umožňuje snadné odpojení celé podsítě od Internetu v případě napadení (zabrání se nejen pokračování případného útoku, ale nedojde ani k šíření případně citlivých interních dat mimo organizaci). Obdobně lze poměrně snadno detekovat a zejména včas zastavit útok z vnějšku tím, že se určité datové toky prostě vypnou.

Přes tato pozitiva je třeba si vždy být vědom i možných negativních důsledků a plné firewally nasazovat pouze na přesně lokalizovaná místa (např. odstínění serverů, které mají poskytovat konkrétní služby a firewall může zajistit, že jiné služby než předem dohodnuté skutečně nebudou poskytnuty). Firewally „on demand“, tedy filtry, které je možno zapnout v případě potřeby, ale v běžném provozu nejsou aktivní, se naopak budou zřejmě více a více stávat součástí standardní funkcionality aktivních prvků počítačové sítě (řada současných směrovačů i přepínačů má již některé funkce firewallů standardně k dispozici).

3 Nejslabší článek – uživatel

Bezpečnou síť si nelze představit bez spolupráce dostatečně poučených uživatelů. Současný trend ve vývoji programového vybavení i samotných operačních systémů směřuje k tomu, aby počítače mohl používat i naprostý laik, s prakticky nulovou znalostí principů funkce. Zdaleka se nejedná pouze o produkty firmy Microsoft, tento trend je dobře patrný i ve vývoji nových prostředí operačního systému Linux (např. Gnome či KDE), v instalačních návodech, které jsou stále jednodušší apod. Rovněž připojení na síť se stává stále snazším a pro uživatele transparentnějším, a to i když používá vytáčenou telefonní linku[6]. Advokáti tohoto přístupu zcela správně

[5] Pojem *imunizace* je zde zcela na místě: lékaři již zjistili, že stejně jako nedostatek hygieny škodí, nebezpečná je i úzkostlivá čistota. Dětem, které vyrůstají v přehnaně čistém prostředí, se nevytvoří dostatečně silná imunitní ochrana (protože nebyla s útoky permanentně konfrontována) a takové děti jsou pak daleko náchylnější na běžné choroby, které u nich mívají podstatně dramatičtější průběh. Na to se často reaguje snahou o ještě větší bezinfekčnost – obdobně jako po překonání firewallu se ozve volání po vztyčení ještě vyšších a nepropustnějších zdí.

[6] Na neznalosti uživatelů v této oblasti vydělávají podvodníci, kteří nabízí speciální služby po stažení jejich jed-

argumentují, že použití počítače se musí stát dostupné každému, ne pouze školeným odborníkům v informatice. Důsledkem je, že na síti jsou připojeny počítače, které v podstatě nikdo neudržuje a jejichž programové vybavení je „děravé“, tj. zpřístupňuje určité služby nebo dokonce celý počítač každému, kdo se o přístup pokusí.

Naštěstí existuje analogie, kterou je řízení motorových vozidel. Stále menší důraz je v této souvislosti kladen na znalosti samotné technologie, zato se ověřuje znalost pravidel provozu. A státy vydávají (a sjednocují) vlastní závazná pravidla, která mimo jiné stanoví i technologické podmínky provozu vozidel. Přitom se nepředpokládá, že by si úpravy a kontroly prováděl samotný uživatel, od toho jsou autorizované provozovny. Obdobně v kontextu bezpečnosti Internetu musíme počítat s tím, že poroste množství explicitně formulovaných pravidel, která budou upravovat chování lidí i vlastnosti systémů na Internet připojených[7]. Uživatelé budou ve stále větší míře povinní se s těmito pravidly nejen seznámit, ale též je dodržovat a nést za případné porušení následky.

Samotná pravidla bezpečného chování na Internetu mohou být přirovnána k základním hygienickým pravidlům: např. „Nevezmeš nemytého ovoce“ je možno převést na „Nespustíš program bez kontroly“. Nepřekvapí proto, že i Masarykova univerzita má soubor pravidel práce na počítačové síti, kde jsou v současné době doplňovány paragrafy týkající se otázek ochrany počítačů před jedním z nejčastějších způsobů napadení v poslední době: před počítačovými viry.

Největší změnu bezpečnosti Internetu přinese právě akceptování faktu, že za tuto bezpečnost odpovídá jeden každý uživatel, a že je v zájmu každého uživatele nejen se s pravidly bezpečného provozu seznámit, ale především je poctivě dodržovat. „Nehygienicky“ se chovající uživatel ohrožuje totiž nejen sama sebe a svá data, ale rovněž ostatní uživatele, neboť jeho počítač může být snadno zneužit k šíření infekce, tedy k útokům na ostatní.

4 Budoucí ohrožení

Zatímco dnes největší mediální reklamu získávají elektronickou poštou šířené viry, s růstem nabízených služeb lze očekávat nová ohrožení a nové způsoby jejich šíření. Zejména lze počítat s postupným růstem využití nejrůznějších webových služeb a systémů, které je zprostředkují – počítačová síť totiž z převážně pasivního přenosového media pomalu přerůstá do mnohem složitějšího systému, v němž jsou nabízeny *služby*, tedy de facto výpočty. Na síti bude v daleko větší míře než doposud nabízena výpočetní kapacita, a tedy i kapacita pro nežádoucí aktivity.

Stane-li se např. jazyk Java či nějaký jeho následník univerzálním programovacím nástrojem Internetu, pak bude samozřejmě významně zjednodušena práce všem, kteří se budou snažit Internet zneužít: bude stačit znalost jednoho jazyka a jednoho prostředí. Obecně snaha o unifikaci, sjednocení s sebou vždy přinese zvýšené nebezpečí zneužití.

5 Závěr

Nelze bohužel očekávat, že by se bezpečnost Internetu v dohledné době zlepšila. Spíše naopak, stále rostoucí dostupnost přináší nové uživatele a mezi nimi se budou vždy objevovat takoví, pro které je Internet hřištěm, na němž musí ukázat svou (pomyslnou) převahu. Jako vždy v podobných bouřlivých časech, tím nejdůležitějším pravidlem je *„Vždy připraven“*. Znamená to, že všichni, kteří Internet jakýmkoliv způsobem používají, musí zvládnout alespoň elementární základy „Internetové sebeobrany“, tedy schopnosti sledovat a vyhodnocovat, co se s jejich počítačem děje, znát základní ochranné mechanismy (dnes jsou to především protivirové programy,

noduchého programu. Ten neudělá nic jiného, než ukončí aktuální telefonní spojení, přes které je uživatel připojen, a okamžitě vytočí nové telefonní číslo – ovšem v zahraničí, s vysokou cenou za minutu připojení. Dobu, po níž byl počítač odpojen, skryje nejčastěji pod nějaký dialog s uživatelem. Následně je zpřístupněna původně nabídnutá služba, ovšem uživatel platí řádově vyšší částky za telefonní spojení – a podvodníci dostávají z této částky svůj podíl.

[7] Dobrým příkladem je ochrana pro spamu, tedy nežádoucí poště: stále přesněji se formulují pravidla, která nebrání přijetí legitimní pošty, ale minimalizují přenos pošty nežádoucí.

na vyšší úrovni pak různé systémy detekce průniku), umět je používat a především umět kriticky a realisticky vyhodnotit informace, které tyto ochranné nástroje poskytují. Přestože tento přístup nemůže garantovat 100 % bezpečnost (podobně, jako zamčený sejf negarantuje, že se do něj nikdo nedostane), na únosnou míru snižuje bezpečnostní riziko a především maximalizuje pravděpodobnost, že v případě napadení toto bude dostatečně rychle detekováno a škody tak minimalizovány. *Tomuto cíli – zvýšení informovanosti a tím i připravenosti všech uživatelů – je věnováno prakticky celé aktuální číslo Zpravodaje ÚVT.* □