Bezpečná síť – nic jednoduššího?

Petr Pištěk, ÚVT MU

S rozvojem celosvětové počítačové sítě jsme svědky trvalého nárůstu bezpečnostních incidentů. Tento trend je patrný jak u problémů, vyvolaných z vnějšku sítě Masarykovy univerzity, tak i u kolizí, primárně způsobených někde po světě počítačem MU. Řešení bezpečnostní problematiky komplikuje především fakt, že každé omezení plné otevřenosti Sítě (pro zvýšení bezpečnosti) znamená v nějaké míře také omezení její funkčnosti pro uživatele. To je vedle stálého rozvoje technologie hlavním důvodem, proč nemůžeme doufat v brzké a definitivní vyřešení otázek bezpečnosti Internetu. Jde spíše o trvalý proces udržování přijatelné míry funkčnosti a bezpečnosti námi ovlivnitelné části sítě při vynaložení únosné míry nákladů. Aktuálním otázkám bezpečnosti sítě Masarykovy univerzity je věnován tento příspěvek.

Základní struktura činností zvyšujících v současné době bezpečnost sítě MU je přibližně následující:

Operativní činnosti

- na koncových zařízeních
- na páteřní síti
- rychlá komunikace mezi ÚVT a LVT

Preventivní činnosti

- aplikace oprav programového vybavení
- antivirová ochrana
- detekční systémy
- omezující systémy
- ochrana hesel
- zabezpečené protokoly
- neanonymní přístup k výpočetní technice

1 Operativní postupy při bezpečnostních incidentech

V organizaci s rozsáhlou počítačovou sítí, jakou MU jistě je, je třeba důkladně optimalizovat postup v případě, že některý z vlastních počítačů začne *ohrožovat* své (blízké, v rámci MU, či vzdálené) okolí. Tato nepříjemná skutečnost se v lepším případě zjistí vlastními detekčními prostředky, v horším pak až ze stížností od správců postižených sítí. V každém případě je třeba pokud možno rychle reagovat, jinak hrozí nebezpečí, že správci dotčených částí Internetu omezí zcela nebo částečně (a na nepředvídatelnou dobu) možnost komunikace s MU. V případě, že nežádoucí aktivita neměla zjevný časově omezený charakter, je třeba především všemi dostupnými prostředky zajistit, aby problémový počítač byl odpojen od sítě, a to v kteroukoliv denní či noční dobu. To dnes ve většině případů prakticky znamená potřebu jeho lokalizace a vypnutí, případně alespoň odpojení od fyzického média (kabelu), např. na straně aktivního síťového prvku. Pak je teprve vhodné se zabývat analýzou příčin a hledáním původce problému. Plánovaná příští generace páteřní sítě MU (tzv. gigabitová páteř, viz článek „Výstavba gigabitové sítě MU“ v minulém čísle Zpravodaje) bude také mít schopnost efektivní filtrace síťového provozu na úrovni jednotlivých IP adres, takže umožní zablokovat transport dat z problémového počítače někde na hranici sítě MU, případně i na hranici sítě fakulty, ještě dříve, než bude fyzicky lokalizován a odpojen. Pro urychlení komunikace mezi ÚVT a fakultními LVT byly vytvořeny elektronické distribuční seznamy ve tvaru `sec-alert@ics.muni.cz` a `sec-alert@<domena-fakulty>.muni.cz`. Jejich smyslem je v co nejkratším možném čase nalézt a informovat na příslušném pracovišti osobu schopnou řešit daný bezpečnostní problém.

2 Prevence bezpečnostních incidentů

Naprostou většinu bezpečnostních incidentů vyvolaných sítí MU způsobily počítače napadené z vnějšku různými typy škodlivých programů – virů, červů (viz článek „Jemný úvod do (anti)virové problematiky“ v tomto čísle Zpravodaje). Je proto logické předcházet těmto událostem tím, že se snažíme průběžně omezovat pole působnosti pro útočníky. Na prvním místě je třeba jmenovat *důslednou aplikaci známých oprav programového vybavení*, zejména pokud se týkají tzv. bezpečnostních děr programových systémů. Tímto způsobem, přes bezpeč-

nostní díru programu Internet Information Server (Microsoft), se např. šířily první verze červa Nimda, který byl tak „úspěšný“ v minulém roce. Počítač s neopravenou známou bezpečnostní dírou (připojený k síti) může být kdykoliv napaden bez sebemenšího přispění jeho majitele a využit útočníkem v různém rozsahu, prakticky dle libosti. Tradiční použití napadeného počítače k dalšímu šíření škodlivého programu je sice nejobvyklejší, ale zdaleka ne nejhorší možnost. Může také například dojít k cílenému získání důvěrných dat z napadeného počítače, k záměrnému poškození dat za nějakým konkrétním účelem, atd. K rychlému šíření informací o nových bezpečnostních problémech programových systémů a jejich řešení (především mezi ÚVT a fakultními LVT) slouží uzavřená diskusní skupina `sec-info@muni.cz`. K průběžné kontrole stavu vlastního počítače ovšem může přispět prakticky každý uživatel. Návod k tomu poskytuje článek „Nenechejte svá okna zastarat“.

Dalším širokým polem pro preventivní činnost je boj proti škodlivým programům, šířícím se pouze s nechtěnou pomocí uživatele – virům. Jejich tvůrci nevynechají žádnou novou technickou možnost, jak šířit svůj zlomyslný výtvor co nejrychleji. Proto se jejich pozornost v poslední době zaměřila na šíření virů elektronickou poštou. Správně totiž vidí jednak komunikační mohutnost Internetu, ale hlavně vystihli jeho slabé místo v podobě koncového uživatele, který, ač proškolen, dychtivě otevře přílohu elektronického dopisu, jehož předmět zní lákavě (byť v cizím jazyce!) nebo jehož odesílatelem je známá důvěryhodná osoba. Úplně zkrátka ale nepřicházejí ani tradičnější metody šíření virů, počínaje disketami a konče např. makroviry v dokumentech (viz článek „Makroviry v dokumentech MS Office“). Proto je nenahraditelným základem antivirové ochrany *funkční a pravidelně udržovaný antivirový program* na každé stanici s operačním systémem Windows (libovolné odrůdy). Je v zájmu každého uživatele, aby si zajistil (podle své odbornosti sám nebo přes svoji fakultní LVT) instalaci antivirového programu na svůj počítač. ÚVT zajišťoval v posledních letech celoškolské licence antivirových systémů za minimální ceny v rámci „promo akcí“ jejich dodavatelů (viz článek „Antiviry pro koncové stanice na MU“). Vzhledem k závažnosti problematiky se zřejmě přejde od letošního roku k výběru stálého dodavatele za standardní cenu. V současné době je již také v provozu doplňkový antivirový systém na centrálním poštovním serveru MU, který by měl pomoci utlumit tlak virů šířených elektronickou poštou (viz článek „Antivirová ochrana v elektronické poště na MU“).

Další možnost, jak nenechat počítačovou síť zcela napospas útočníkům, poskytují tzv. *detekční systémy* (Intrusion Detection System, IDS). Jejich činnost spočívá v průběžné analýze veškerého síťového provozu na koncové stanici nebo na segmentu sítě, v upozornění na aktivity, které detekční systém považuje za nestandardní nebo přímo nebezpečné, a v případné obranné reakci na zjištěné události. ÚVT má k dispozici systém firmy NetworkICE, který se osvědčil zvláště při odhalování počítačů MU, napadených červem Code Red a jeho následníky. Nasazení detekčního systému ovšem vyžaduje příslušnou organizaci sběru a analýzy varovných zpráv, aby se soustřeďovaly u kvalifikovaných pracovníků s dostatečnou časovou kapacitou na jejich rozbor.

Části počítačové sítě, které vyžadují zvýšenou ochranu a přitom mají ze své povahy zúžené spektrum potřebných protokolů (typicky servery klíčových informačních systémů), bývá obvyklé a vhodné chránit systémy omezujícími provoz (např. filtrujícími datové pakety), tzv. *firewally*. Jejich základní funkcí je zpravidla zamezit transportu dat mimo vybrané uzly a protokoly. Na MU jsou nasazeny k ochraně centrálních serverů informačních systémů a v sítích fakult podle úvahy a potřeby lokálních správců.

Významným prvkem preventivního udržování bezpečnosti v síti MU je *ochrana přístupových hesel*. Ta začíná především tím, že každý uživatel dodržuje mnohokrát opakované (a stále porušované) zásady – nepoužívá pro heslo triviální ani snadno odhadnutelné výrazy, nepíše si hesla na rám monitoru ani je neponechává volně na pracovním stole, nesděluje je na potkání známým, tím méně neznámým.

Dále je nezbytné se v rámci technických možností programového vybavení zbavit používání „klasických“ funkcí a protokolů, které posílají

po síti hesla v otevřené (nešifrované) podobě a začít používat *bezpečné klientské programy* na všech koncových stanicích. Pro základní síťové aplikace typu telnet, ftp, el.pošta existují jejich varianty, pracující se zabezpečenými protokoly, minimálně bez posílání otevřených hesel (viz článek „Zabezpečené spojení se vzdáleným počítačem“). Důležitým přínosem pro bezpečnost sítě bude také postupné (v rámci finančních možností) odbourání klasických sdílených segmentů ethernetu a *přechod na přepínané technologie*, u kterých je významně redukována možnost nežádoucího sledování provozu cizích počítačů.

Z úvah o prevenci možných bezpečnostních incidentů v síti MU nemůžeme vynechat ani události způsobené úmyslným protiprávním jednáním. Zde se jednoznačně osvědčuje dodržovat důsledný postup ke zjištění původce každého takového incidentu. Tomu napomáhají především organizační a technická opatření k *odbourání anonymního užívání výpočetní techniky* na MU. Přitom je žádoucí v rámci technických a finančních možností postupně zavádět spíše technická opatření (např. zpřístupnění počítačů v učebnách a studovnách na základě přihlášení jménem a heslem z centrální databáze), která jsou méně náchylná k chybám a která zvyšují pocit odpovědnosti u přihlášeného uživatele. Za připomenutí stojí rovněž existence závazných směrnic MU pro užívání počítačové sítě (viz např. `http://www.ics.muni.cz/techinfo/`), které právně zakotvují *povinnosti uživatelů sítě* a současně poskytují řadu užitečných praktických pokynů. Bezpečnost je totiž záležitostí nejen správců, ale i všech koncových uživatelů. □