

Spam a viry se vzájemně podporují

Mirek Holý

V současné době se stále častěji objevuje i v neoborných médiích problematika spamu a virů. Přestože technicky jde o dvě rozdílné záležitosti, pozadí obou často splývá. Jsme svědky rozesílání nevyžádaných e-mailů, které obsahují viry, a naopak se šíří viry, které připravují prostředí pro rozesílání spamu z napadených systémů. Společným jmenovatelem obou je velmi často kriminální pozadí. Dalším společným znakem je poškozování legálního byznysu.

Spam

Jde o nevyžádané sdělení často s komerční nabídkou, které je dáno na vědomí mase uživatelů. Zdaleka nejčastěji se šíří prostřednictvím zpráv elektronické pošty. Můžeme se s ním ale setkat i v diskusních skupinách. Většina spamu se dá rozdělit podle povahy obsahu do tří následujících kategorií:

- komerční nabídka konkrétního výrobku,
- upozornění na internetový projekt (např. pornografický web),
- distribuce virů či upozornění na zákeřně upravené WWW stránky.

Jakým způsobem spam zvyšuje náklady?

Protože se spam šíří především elektronickou poštou, jsou zaměstnanci nuceni zpracovávat větší množství zpráv. Vždy se nedá již ze subjektu zprávy určit, zda jde o spam, či legální zprávu. Musí se vyhodnotit

obsah, což ještě prodlužuje dobu strávenou neefektivní činností spojenou s vyhodnocováním, zda se jedná, nebo nejedná o zprávu s užitečnými informacemi.

Kromě času zaměstnanců stráveného nad vyhodnocováním zpráv elektrické pošty mohou organizaci vzniknout i další náklady spojené s odstraňováním škod spojených s činností virů, které do organizace mohou proklouznout právě prostřednictvím hromadně se šířících zákeřných zpráv elektrické pošty.

Dalším způsobem, jakým spam sahá do kapsy svých příjemců, je zvýšená potřeba výkonu infrastruktury zajišťující zpracování příchozích zpráv elektronické pošty.

Jaký je podíl spamu v celkové počtu e-mailů?

Existují velké rozdíly mezi jednotlivými zeměmi. Zdaleka nejvíce jsou postiženi uživatelé v anglicky hovořících zemích.

Především USA, které vzhledem k velikosti trhu a velkému rozšíření informačních technologií v populaci představují pro spamery atraktivní působiště.

Společnost MessageLabs, která se celosvětově věnuje problematice spamu, zaznamenala v květnu 2004 z celkové počtu 909 milionů vyhodnocených zpráv elektronické pošty 76 % spamu a 9,1 % zpráv obsahovalo vir. Ze závěrů dubnového průzkumu stejné společnosti zveřejněných na stránkách theregister.co.uk vyplývá, že zatímco v USA činil podíl spamu 83 %, v Nizozemí se jednalo „pouze“ o 30 %.

Odkud se spam rozesílá?

Vzhledem k větší důslednosti administrátorů v poslední době a ke skutečnosti, že existují seznamy serverů, které spam rozesílají, což dovoluje systémům přijímajícím e-mail spam filtrovat podle odesílatele, volí spammeri často možnost spam

Inzerce




Tridion R5 kompletní řešení pro Web Content Management

- Tvorba
- Správa
- Distribuce
- Publikování webového obsahu

KOMIX s.r.o., Holubova 1, 150 00 Praha 5, tel.: +420 225 989 811, www.komix.cz

rozesílat z velkého množství tzv. botů. Jde o počítače infikované typem viru, který dovoluje jejich vzdálené ovládnutí a odesílání pošty, aniž by si toho uživatel všiml. Celé sítě botů jsou tvořeny a následně spammerům prodávány na černém trhu. Velmi často jsou s tvorbou botů zmiňováni především hackeři z Ruska.

Jak se bránit

V prvé řadě je dobré si vážít své adresy elektronické pošty a zbytečně ji v textové podobě nevystavovat na webových stránkách, tam se pro roboty spammerů hledající e-mailové adresy stane jednoduchou kořistí.

Dalším způsobem obrany je vhodné technické řešení zaměřené především na restriktivní nastavení poštovního serveru a filtrování pošty na přítomnost spamu. K filtrování lze použít komerční i zdarma dostupný software. V prostředí podnikových sítí se vyplatí nasazení především síťových antispamových bran. Vzhledem k možnosti vytvořit kvalitní antispamové řešení pomocí zdarma dostupného software nemusí být rozpočet IT oddělení v nákladových položkách jeho realizaci viditelně narušen.

Pravděpodobně právě proto, že nejvíce jsou působením spammerů zasázeny USA, vznikl a byl přijat první zákon postihující spammery právě zde (CAN-SPAM). Naši zákonodárci ovšem nestojí stranou. Vládní návrh zákona o službách informační společnosti již schválila poslanecká sněmovna. Zákon mimo jiné počítá až s desetimilionovou pokutou pro odesílatele spamu.

Prolínání problematiky spamu a virů

Jak již jsem naznačil v úvodu článku, existují typy virů, tzv. e-mailové červy, šířící se z počítače na počítač prostřednictvím zpráv elektronické pošty. Červ na napadeném systému zjistí používané e-mailové adresy a na ně, často prostřednictvím vlastního SMTP engine, posílá zprávy obsahující jeho další inkarnace. Jinou možností, jak elektronická pošta rozesílaná ve velkém může napomoci šíření zákeřných programů, je rozeslání e-mailů s odkazem na webové stránky obsahující zákeřný kód. Ano, i prostřednictvím pouhé návštěvy takto upravených stránek může dojít k infikování systému virem nebo například k uživatelem nechtěné instalaci reklamního software.

O sítích botů jsem se již zmínil. Tady jde o opačný případ, viry připravují půdu pro

odesílání spamu ve velkém. Uvádí se, že až 80 % spamu je rozesíláno právě ze sítí botů.

Dopady činnosti virů na fungování podniku

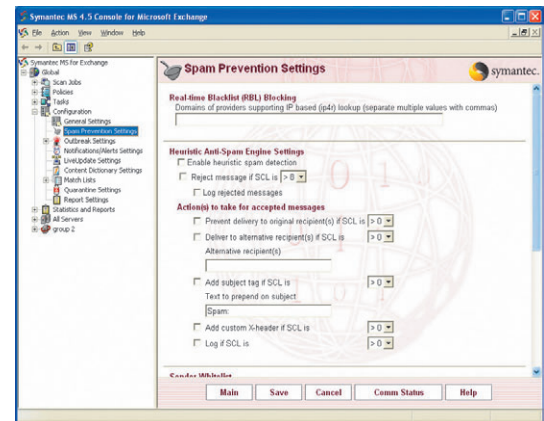
Ztráty mohou organizaci vzniknout narušením průběhu některých procesů v důsledku omezení funkčnosti nebo nedostupnosti infikovaných aplikací nebo aplikací provozovaných na napadené platformě. Pokud jde o hlavní procesy, může být situace vážná. V této souvislosti zmíním případ finské banky Sampo, která ve strachu z náklady virem Sasser zavřela na několik hodin všech svých 130 poboček. Navýšení nákladů vzniká také zvýšenými nároky na spotřebu lidských zdrojů při zavedení provizorního nebo havarijního provozu v důsledku činnosti virů.

Další vážnou hrozbou je možnost úniku citlivých, případně tajných informací mimo organizaci. Některé viry jsou schopny zpětně komunikovat, čehož se často využívá ke krádeži autentizačních údajů. Obdobným způsobem je možné provést cílený útok na získání konkrétních dat.

Obrana proti virům

Organizace se zvýšenou potřebou bezpečnosti by se neměly spoléhat pouze na jednoúrovňovou antivirovou ochranu. Odlišné detekční postupy různých výrobců antivirových produktů mohou prokázat svoji opodstatněnost především v případě cíleného útoku, který může být proveden pomocí nerozšířeného nebo značně modifikovaného, tj. předem neprozkoumaného, zákeřného programu. V praxi se víceúrovňová antivirová obrana realizuje nejčastěji prostřednictvím síťové antivirové brány a personálních antivirových systémů na uživatelských stanicích. Každá úroveň je založena na technologii jiného výrobce. Mezi další zařízení, která přispívají k ochraně před virovou infekcí, patří firewall a systémy detekce a prevence narušení. Firewall znemožní potenciální infekci přes nepovolené služby. Systémy detekce a prevence narušení upozorní na nestandardní stavy, které mohou být způsobeny právě činností virů, případně přímo viry detekují a dle své konfigurace reagují.

Mimo technických prostředků jsou důležitá příslušná opatření na úrovni řízení, která jsou zanesena v bezpečnostní politice organizace. Krom známých pouček typu „v podezřelém e-mailu na nic neklikat“ je užitečné definovat i procesy zajišťující včasnou informovanost bezpečnostních pracovníků, protože řada nových virů



zneužívá právě objevené zranitelnosti operačních systémů a aplikací. Často je tudíž nejlepší obranou včasné záplatování, nebo včasná adekvátní reakce na právě oznámenou zranitelnost.

e-mail: system@ccb.cz
www.SystemOnLine.cz

Autor článku, Mirek Holý, působí ve společnosti Actinet Informační systémy.

www.symantec.cz
tel.: +420 233 101 555