Počítačové viry, antivirová ochrana a bezpečnost na internetu

Počítačové viry

Počítačový vir není nic jiného než „pouhý“ program. Na rozdíl od většiny programů, které se snaží uživatelům zjednodušovat a ulehčovat práci, počítačový vir se snaží o opak – zmást uživatele, způsobit nefunkčnost vybraných programů a v tom nejhorším případě smazat cenná data nebo rovnou celý disk. Hlavní charakteristikou počítačového viru je však jeho snaha se šířit. Vytvářet další svoje kopie a šířit se jak mezi počítači, tak i případně v rámci jednoho PC. Virus musí sám sebe replikovat a provádět další svoji činnost.

Pravé viry tvoří jen jednu z mnoha podkategorií spadajících pod pojem „Malware“ (Malicious Software – zákeřný, škodlivý, …. software).

Historie virů

Historie počítačových virů začíná na počátku osmdesátých let, což je ve výpočetní technice poměrně dávná minulost. V roce 1983 sestrojil Dr. Frederick Cohen první samomnožící program, který se začal označovat jako vir. Jednalo se o neškodný kód, jenž se uměl pouze sám množit. První „škodlivý“ vir s názvem Bram naprogramovali v roce 1986 bratři Basid a Amjad Farooq Alvi. Tím odstartovali boom nepopulárních programů – počítačových virů. Bram byl oproti některým dnešním virům pouhým pohlazením, protože autoři virů znají a předávají si mezi sebou moderní techniky, které umožňují virům měnit svůj vlastní kód, ukrývají se před antivirovými programy a disponují spoustou dalších „triků“.

Počítačový vir je program, který je schopen se bez vědomí uživatele množit a provádět nežádoucí operace. Protože z každého zavirovaného programu může být nakaženo mnoho dalších programů, připomíná množení viru řetězovou reakci. Každý vir, ať už se jedná o jakýkoliv typ, je svým způsobem nebezpečný a pochopitelně v počítači nežádoucí. K jeho zlikvidování existují takzvané antivirové programy, které vir dokáží vyhledat a odstranit.

Je jasné, že žádný antivirový program není a ani nemůže být dokonalý tak, aby nalezl všechny viry, které v daném okamžiku existují. Každý antivirový program je za novými viry pozadu, protože aby mohla existovat antivirová ochrana, musí vir nejprve vzniknout a rozšířit se. Na každý vir lze nalézt metodu jak jej odstranit, hlavní ale je jak dlouho to potrvá a jak se stihne vir rozšířit.

Jak se viry šíří

Pro své šíření potřebuje vir jednak prostředí, které zná – operační systém – a pak takové typy souborů, které mu šíření dovolují – většinou spustitelné programy. Viry se mohou šířit prostřednictvím následujících metod:

Spustitelné soubory (programy) – bezesporu jeden z nejčastějších případů šířeni virů. Vir se při spuštění programu nahraje do paměti a poté provádí svou „nekalou“ činnost (šíří se a ničí). Nákaza hrozí u souborů s koncovkou EXE, COM, SYS, DLL, SRC, a spousty další. Virus je buď celý samotný soubor, nebo jen část kódu souboru. V tomto druhém případě dojde k přepsání kódu „běžného“ souboru kódem viru.

Dokumenty – makroviry. Vir se uloží přímo do dokumentu, který může obsahovat makra (např. Word nebo Excel). Makro se pak spustí při otevření souboru a vir může začít provádět svoji činnost. V zásadě tak může být virus i v jiných typech souborů, které neobsahují pouze data, ale i aktivní kód.

Elektronická pošta (e-mail) – velmi moderní a v poslední době bohužel častý případ virových „invazí‘. Vir je přenášen jako (samospustitelná) příloha e-mailu, takže jakmile dojde nová zpráva, stačí ji pouze otevřít a vir se aktivuje.

WWW stánky s aktivním obsahem (skripty apod.) mohou také být zdrojem virů.

Systémové oblasti – cílem viru v tomto případě je bootsektor nebo partition tabulka. Jedná se o oblasti, do kterých za normálních okolností nemá uživatel přístup a které slouží pouze systému. Virus tak i po odstranění napadených souborů v PC zůstává a při načtení systému se může opět začít šířit.

Typy virů

Podle toho, jakým způsobem viry pracují a jak se projevují, je lze rozčlenit do několika základních skupin:

Bootviry

Jak již sám název kategorie virů napovídá, jedná se o viry, které mají spojitost se zaváděním systému (bootováním). Vir napadne bootsektor (většinou 1. sektor na disku) nebo partition tabulku pevného disku či diskety. Při zavádění systému je pak pohodlně aktivován a převezme kontrolu nad funkcemi systému. Jestliže vir obsadil partition tabulku, následně její obsah bezpečně uloží a vzhledem k systému, resp. požadavkům softwaru se partition tabulka jeví v pořádku.

Vir se šíří prostřednictvím bootsektoru disket. Aby byl počítač takovým virem napaden, musí se z nakažené diskety nabootovat (např. necháme-li v disketové mechanice nakaženou disketu a počítač spustíme). Byl to častý druh virů v 80. letech.

Souborové viry

Souborové viry napadají pouze soubory. Jedná se o kapitolu virů, které se projevují nejrozmanitějším způsobem. Podle toho se dále dělí:

- Přepisující vir – přepíše část programu, který napadl vlastním kódem. Díky tomu je velmi nápadný, a proto nemá mnoho šancí se rozmnožit.
- Link vir – „přilepí“ se (přilinkuje) k napadenému souboru, což umožní chod programu a zároveň činnost viru.
- Doprovodný vir – zkopíruje napadený soubor do souboru se stejným jménem, ale typu COM, a k tomu se připojí (vzniknou dva soubory, kde COM je nakažený). Vir využívá vlastnosti OS MS-DOS, jenž nejprve spouští COM soubory.
- Vir přímé akce – provede destrukční akci a tím skončí. Například smaže celý disk a tím „zabije“ sám sebe.
- Rezidentní vir – načte se a drží v paměti a tím snadno napadne soubory, se kterými se pracuje.
- Stealth vir – vir s touto vlastností se umí načíst do paměti a kontroluje činnost systému. Pokud antivirový program kontroluje zavirovaný soubor, pak mu vir s touto vlastností vrátí kód před infekcí. Pro antivirové programy, jež nejsou vybaveny anti-stealth kontrolou, je vir prakticky nezjistitelný.
- Zakódovaný vir – je zakódován určitým proměnným algoritmem, takže jeho tělo je pokaždé jiné. Stejná je pouze dekódovací instrukce.
- Polymorfní vir – podobný jako předchozí. Pro každý napadený soubor se kóduje jinak a vytváří i jinou dekódovací funkci. Takový vir nemá v žádném okamžiku v žádném z napadených souborů stejnou sekvenci svého kódu.

- Metamorfní vir – obsahuje funkci, která při kopírování sebe sama kompletně přepíše a vir tak vypadá úplně jinak. Tento mechanismus je poměrně složitý a celá replikační funkce zabírá až 90 procent kódu viru.
- Fast infektor – šíří se extrémně rychle díky tornu, že napadá soubory při spuštění i při jakékoliv manipulaci s nimi. Snadno se rozšíří a tím na sebe upozorní.
- Slow infektor – na rozdíl od předchozího se šíří velmi pomalu a opatrně.

Multipartitní viry

Bootviry se aktivují ihned při zavádění systému, ale k infekci se musí nabootovat z nakažené diskety, což jejich šíření omezuje. Souborové viry se šíří prostřednictvím souborů, což je pro jejich šíření výhodné, ale potřebují být aktivovány spuštěním. Kombinací a výhod obou typů virů využívají tzv. multipartitní viry. Infikují partition tabulku i soubory.

Makroviry

Makroviry se objevily až s příchodem makrojazyků především v textových editorech a tabulkových procesorech. Zákeřnost makroviru spočívá vtom, že vir je přenášen a uložen v dokumentu.

Nebezpečí makroviru spočívá vtom, že ovládne program i šablony a poté při určité operaci (například uložení souboru) bude spuštěno makro s destrukčními účinky (např. vymazání dokumentů).

Trojský kůň a červ

Zde se nejedná přímo o druh viru, ale spíše o metodu jeho šíření. V běžném jazyce se ale ustálily i tyto pojmy jako typy virů.

Trojský kůň (trojan horse) je program, který se zdá být něčím jiným (užitečným, zajímavým), ale ve skutečnosti provádí škodlivou činnost. Například se vydává za spořič obrazovky a mezitím maže soubory na disku. Trojský kůň také může umožňovat přístup k PC útočníkovi. Ve své podstatě se obecně nejedná o virus, protože se sám nešíří.

Červ (worm) je programový kód, který se šíří sám prostřednictvím počítačové sítě. K tomuto účelu na rozdíl od klasických virů nemusí využívat souboru (respektive jich využívá odlišným způsobem). Po celé síti se šíří díky bezpečnostním nedostatkům a často ke svému šíření využije souboru. Celý soubor je ale pak možno považovat za červa.

Jak se viry prakticky projevují

Počítačový vir je program a jako takový se projevuje podle toho, jak byl naprogramován. Existují stovky způsobů, jak se viry projevují, počínaje výpisem nejrůznějších humorných hlášení na obrazovku až po destrukční viry. Obecně můžeme projevy virů rozdělit na:

Obtěžující

Příznaky obtěžujících virů spočívají například ve výpisech nesmyslných hlášení na obrazovku, která se zpočátku mohou zdát humorná, ale pokud každých 5 minut počítač napíše, že je unavený,

pak uživatel asi dlouho s nervy nevydrží. Viry mohou obtěžovat také záměnou kláves na klávesnici, takže něco jiného píšete a něco jiného se zobrazuje na obrazovce. Některé obtěžující viry zjistí, že je k počítači připojen modem, a klidně zavolají třeba na číslo 906… Při placení účtu se nepřestanete divit. Fantazie programátorů takových typů virů je prakticky neomezená.

Destrukční

Destrukční viry vzbuzují určitý respekt již při vyslovení této kategorie. Základním úkolem takových virů je zlikvidovat data. Chytré viry pracují tak, že nezničí všechna data na disku, ale postupně zaměňují pouze určité byty nebo řetězce. Uživatel takový vir těžko odhalí a při dlouhodobém působení nakazí i záložní kopie. Jednoduché viry zničí okamžitě po napadení například obsah disku a tím vlastně zničí samy sebe.

Destrukční viry, stejně jako obtěžující, mohou být naprogramovány na určitou dobu (například pátek třináctého) nebo v souvislosti s určitou akcí v počítači. Také mohou být zaměřeny pouze na určitý typ dat (např. dokumenty MS Office).

Ostatní

Sem se řadí ostatní typy virů. Často se stává, že viry nejsou kvalitně napsané a že se dostávají do kolizí s jinými programy. Pak se z původně neškodného viru klidně může stát destrukční – a to vlastně náhodou.

Spousta virů nevykonává žádnou přímo destrukční činnost, ale pouze se snaží dále a dále šířit. I takové viry mohou způsobovat problémy, obsazovat paměť, brzdit síťový provoz a podobně.

Další viry mohou rozesílat informace z vašeho počítače na jiné, kde si je může autor viru přečíst, šířit se automatickým rozesíláním elektronickou poštou, nebo třeba šifrovat data na disku.

Proč viry?

Viry podobně jako i jiný malware vznikají ze spousty důvodů. Každopádně je tvoří vždy programátoři, nebo alespoň lidé využívající některý z programů přímo určený ke generování virů. Samotný vznik konkrétního viru může mít spoustu důvodů. Některé vznikají jako snaha zviditelnit se, jako výzkumný projekt, vandalismus, snaha někoho poškodit nebo vydírat.

Antivirová ochrana

Antivirové programy

Proti virům je třeba se bránit. V dnešní době si již nemůže být jistý žádný uživatel počítače, který datově komunikuje alespoň částečně se svým okolím. Kromě opatrnosti jsou silným prostředkem proti virům antivirové programy. Dokáží nejen najít vir, ale někdy i „vyléčit nakažený soubor tak, že po zásahu antivirového programu funguje správně a nemusí být celý smazán.

Na softwarovém poli působí poměrně velké množství antivirových programů. Antivirový program by měl používat každý, kdo je alespoň částečně nucen komunikovat prostřednictvím disket nebo jiného typu média s daty na jiných počítačích a kdo je propojen do sítě s jinými počítači. Antivirovou kontrolu by měl uživatel provádět v pravidelných intervalech. Důležitá je také

aktualizace virové databáze – načtení nově zjištěných virů do databáze antivirového programu je nutné proto, aby antivirový program byl schopen nové viry identifikovat a odstranit. Aktualizace se provádí většinou přes internet, může být však ještě realizována pomocí disket nebo CD. Virus bez aktuální virové databáze je většinou téměř k ničemu, protože nedokáže zachytit novější viry (které se také nejvíce šíří.)

Některé antivirové programy:

NOD32
Avast!
AVG
Kaspersky AV
Norton AV
…..

Informace o virech a antivirových produktech nalezneme např. na stránkách výrobce nebo na některých serverech zaměřených na virovou problematiku (třeba www.viry.cz)

Jak pracují antivirové programy

Současné antivirové programy používají různé techniky. Asi nejstarší a nejznámější je technika vyhledávání prostřednictvím vyhledávací sekvence. Většina virů má určitou specifickou sekvenci, podle které lze vir jednoznačně specifikovat (Al 00 10 85 C2 00). Vir prohledává celý disk a soubory s takovou instrukcí označí za napadené. Při tvorbě antivirových programů je velmi obtížné najít takovou sekvenci viru, která zároveň není obsažena v žádném programu v počítači, protože by docházelo k falešným odhalením – antivirový program by mohl „falešně“ považovat čistý program za vir.

Bohužel, programátoři virů znají antivirové techniky a snaží se vyhledávací metodu obejít. Velmi obtížné je hledání tzv. polymorfního viru, který mění svůj vlastní kód. První polymorfní viry se samy kódovaly, ale měly alespoň krátkou dekódovací instrukci, podle níž je bylo možné vyhledávací metodou odstranit. Dnešní polymorfní viry již umí průběžně měnit i dekódovací instrukci, takže jejich tělo může být v počítači několikrát, ale pokaždé vypadají jinak. Takové viry jsou pak prostřednictvím vyhledávací instrukce nezjistitelně. I tuto lest programátoři antivirových programů zvládli. Antivirový program v sobě obsahuje emulátor strojového kódu, který dokáže rozbalit zakódovaný vir. Naprogramovat takovou instrukci je velmi obtížné, zvlášť když je vir pokaždé zašifrován jinak.

Na rozdíl od pouhé detekce viru heuristická analýza sleduje programy tak, že emuluje (nahrazuje) instrukce programu, resp. zjišťuje, co sledovaný program s počítačem provádí, a na základě zjištění vyhodnotí, zda je to v pořádku, či nikoliv („spustí program pod svou kontrolou“). Napsat takový emulátor je velmi obtížné, ale pokud je naprogramován skutečně dobře, dokáže najít 70% nových neznámých virů.

Jednou z dalších technik antivirových programů je tzv. kontrola integrity. Antivirový program s testem integrity hlídá změny v systému, adresářích a systémových oblastech disku a na základě změn detekuje vir. Tato metoda je velmi spolehlivá, ale neumí zjistit konkrétní vir, pouze změnu v systému.

Každá technika má své silné a slabé stránky. Antivirové programy proto většinou používají kombinaci technik a tím zvyšují svou účinnost.

Antivirové systémy obsahují tzv. on-access scanner (rezidentní část antiviru), který skenuje programy při spouštění a při přenosech. Obsahuje scanner příchozí i odchozí elektronické pošty. Na vyžádání uživatele umožňuje samozřejmě provést hloubkovou kontrolu systému nebo určitých oblastí a automaticky se aktualizuje (nejlépe po internetu).

Internet – nový druh virového nebezpečí

V souvislosti s největší počítačovou sítí na světě – internetem – je možné obávat se napadení virem dvěma způsoby:

Stáhnutím nakaženého programu či souboru

Internet je kromě obrovské spousty informací i velkým zdrojem virů. Nikdy nemůžete vědět, zda program nebo soubor uložený na internetu není nakažen virem. Pokud stahujete z internetu program, před spuštěním jej v každém případě zkontrolujte antivirovým programem. Antivirový program se zapnutou rezidentní ochranou by měl toto provést automaticky.

Před stahováním zejména programů do počítače je dobré ověřit, z jakého serveru je soubor stahován. Je pochopitelné, že servery velkých a „ověřených“ firem si těžko dovolí dát na své stránky zavirovaný soubor. I známé freewarové servery většinou neobsahují linky na přímo zavirované programy. Problém je hlavně u neznámých a pochybných serverech (obzvláště s tématikou warez, porno apod.)

Infikovaný e-mail

Bohužel, v poslední době se forma nakažených e-mailů stává jedním z nejnebezpečnějších typů virů vůbec. „Kvalitní“ e-mailový vir je zákeřný v tom, že ani nemusíte vědět, kdy a že vůbec jste jej dostali. Přijde „zabalený“ v běžné zprávě (e-mailu) a už pouhým otevřením takové zprávy dojde k aktivací viru a infikaci počítače. Problém je v tom, že nemáte možnost poznat, zda je právě tato zpráva zavirovaná, či nikoliv, protože jediným vodítkem je odesílatel a předmět zprávy. Obvykle když zprávu otevřete, abyste zjistili její obsah, pak – pokud se jedná o vir – je okamžitě po otevření rozeslán na všechny další adresy, které nalezl v seznamu adres (například v Outlooku) – tím nechtěně zavirujete e-maily i všem, se kterými jste dosud komunikovali elektronickou poštou.

Jak bojovat proti virům

- Mějte nainstalovaný kvalitní antivirový systém
- Udržujte antivirový systém aktualizovaný (databázi i program)
- Mějte v antivirovém systému zapnutou rezidentní ochranu
- Každou neznámou disketu, kterou vkládáte do svého počítače, nejprve otestujte antivirovým programem.
- Nepouštějte ke svému počítači nedůvěryhodnou cizí osobu
- Pravidelně zálohujte svá data. Pokud totiž vir zlikviduje celý disk, nic až tak vážného se nestane, jestliže máte důležitá data zálohována.
- Buďte obezřetní. Většina virů se nějak projevuje. Ať je to delším zaváděním systému, podezřelým padáním programů, nebo jiným „neobvyklým“ chováním.
- Soubory stažené z internetu před spuštěním zkontrolujte antivirovým programem.
- Podezřelou či nevyžádanou e-mailovou poštu z internetu ani neotevírejte a ihned mažte.
- Otevřete-li e-mail a zjistíte, že obsahuje soubor, který by tam být neměl nebo má „divný“ název či koncovku, zavřete tento e-mail a smažte jej.

Bezpečnost na internetu

Malware

Malicious Software zahrnuje kromě samotných virů spoustu dalších typů programů, jejichž výskyt v počítači je nežádoucí. Podíváme se tedy na další pojmy a typy této počítačové „havěti“ se kterou se můžeme běžně setkat.

Spyware

Spyware je program, který využívá Internetu k odesílání dat z počítače bez vědomí jeho uživatele. Narozdíl od backdooru jsou odcizovány pouze „statistická“ data jako přehled navštívených stránek či nainstalovaných programů. Tato činnost bývá odůvodňována snahou zjistit potřeby nebo zájmy uživatele a tyto informace využít pro cílenou reklamu. Nikdo však nedokáže zaručit, že informace nebo tato technologie nemůže být zneužita. Proto je spousta uživatelů rozhořčena samotnou existencí a legálností spyware. Důležitým poznatkem je, že spyware se šíří společně s řadou sharewarových programů a jejich autoři o této skutečnosti vědí. [www.viry.cz]

Adware

Obvykle jde o produkt, který znepříjemňuje práci s PC reklamou. Typickým příznakem jsou „vyskakující“ pop-up reklamní okna během surfování, společně s vnucováním stránek (např. výchozí stránka Internet Exploreru), o které nemá uživatel zájem. Část Adware je doprovázena tzv. „EULA“ - End User License Agreement – licenčním ujednáním. Uživatel tak v řadě případů musí souhlasit s instalací. Adware může být součástí některých produktů. Ačkoliv nás reklama doprovází během celé činnosti s daným programem, odměnou je větší množství funkcí, které nejsou v klasické free verzi (bez reklamy) dostupné. [www.viry.cz]

Dialer

Dialer je program, který změní způsob přístupu na Internet prostřednictvím modemu. Místo běžného telefonního čísla pro Internetové připojení přesměruje vytáčení na čísla se zvláštní tarifikací, např. 60 Kč / minutu (tzv. „žluté linky“). V některých případech se tak děje zcela nenápadně nebo dokonce automaticky, zvlášť když oběť používá špatně nastavený, popř. „děravý“ internetový prohlížeč. Dialer může být na PC vypuštěn návštěvou „nevhodné stránky“ (např. pornografické), například za využití technologie ActiveX, takže problémy mohou nastat především uživatelům Internet Exploreru. V jiném případě může jít o nenápadný spustitelný soubor (.EXE), který je nic netušícímu uživateli vnucován ke stažení klasickým dialogem (mluvíme-li o prohlížeči Internet Explorer). [www.viry.cz]

SPAM

Spam je nevyžádané masově šířené sdělení (nejčastěji reklamní) šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging.

E-mailové adresy do spamových databází jsou získávány mj. pomocí robotů, které procházejí webové stránky a sbírají e-mailové adresy na nich uvedené. Také registrací na některých serverech s uvedením vaší adresy je možné přidat se na seznam pro spam. No a samozřejmě viry na PC mohou odeslat seznam vašich kontaktů nebo přímo odesílat spam z vaší adresy.

Backdoor, Zombie, Botnets

Některé viry (červy) často jako svojí další činnost instalují do PC tzv. Backdoor (zadní vrátka), které umožní k systému přístup útočníkovi. Z takto nakaženého PC může být vytvořena „zombie“ pod kontrolou autora viru. Sítě takových strojů se nazývají botnets a často jsou využívány k další nekalé činnosti jako je např. odesílání spamu nebo provádění DDoS (Distributed Denial of Service) útoků.

Hoax

Anglické slovo HOAX v překladu znamená: Falešnou zprávu, Mystifikaci, Novinářskou kachnu, Podvod, Poplašnou zprávu, Výmysl, Žert, kanadský žertík. V počítačovém světě slovem HOAX nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečným virem nebo podobnou havětí, ale i další fámy, petice, výstrahy, pyramidové hry, řetězové dopisy apod. Jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to s největší pravděpodobností HOAX. Takové zprávy obtěžují příjemce, zbytečně zatěžují linky a vyzrazuje informace (e-mailové adresy), čehož se dá dále využít pro spam. [www.hoax.cz]

Phishing

Phishing je činnost, při které je rozesílán email uživatelům Internetu, který se tváří, že byl odeslán z legitimní organizace (většinou finanční, banky apod.). Předmětem takového emailu je získat osobni informace uživatele, zejména pak čísla platebních karet a jejich PIN a následně jejich zneužití. Phishing email obsahuje často odkaz na stránky s formulářem, který uživatel v dobré víře vyplní a odešle. Odeslaná data vsak nekonči u bankovního či finančního ústavu, ale v rukou tvůrce phishing emailu.

Další

Kromě těchto existují i další pojmy v oblasti. Rootkit je program maskující svoji přítomnost svojí co nejhlubší infiltrací do operačního systému, keylogger (nebo jiný logger) zase zaznamenává činnost na PC a k informacím umožní přístup útočníku. Čas od času se objevují další pojmy ukazující na jiný typ či podtyp podobných programů.

Obrana:

- používat šedou kůru mozkovou
- používat antiviry, antispyware, anti….,
- používat alternativní prohlížeče, programy, OS
- nechodit na stránky s podezřelým obsahem (nelegální: sw, pornografie, cracky, ...)
- být paranoidní

Bezpečnost sítí

Dokud byly počítače pouze samostatné stanice, existovalo hlavně nebezpečí virů a to zanesených z infikovaných médií. Jsou-li však počítače připojeny do počítačové sítě nebezpečí vzrůstá a s přístupem k internetu jsme prakticky stále v potenciálním ohrožení.

Firewall

Jako obrana proti nebezpečí ze sítě existuje firewall. Hned na úvod je třeba říci, že nenahrazuje antivirový program, antispyware a další, ale v kombinaci nám dovolí mnohem lépe ochránit náš systém.
V počítačové terminologii se firewallem nazývá software či hardware (hardwarové firewally), jehož funkcí je kontrolovat (povolovat či zakazovat) komunikaci v počítačové síti na základě daných pravidel. Používá se na oddělování různých částí sítě (nejčastěji odděluje nebezpečný internet od místní sítě).

Osobní firewall je firewall určený pro ochranu pracovní stanice (tedy jednoho počítače). Jedná se tedy o software (aplikaci) s přívětivým ovládáním, tak aby s ním mohl pracovat i méně zkušený uživatel. Z funkčního hlediska pracuje velmi podobně – odděluje počítač od sítě. Navíc, díky tomu, že běží přímo na pracovní stanici, může kontrolovat komunikaci více detailněji (může kontrolovat, které aplikace komunikují) než firewall chránící celou síť (protože neběží na tomto počítači, nemá možnost zjistit, ke které aplikaci komunikace patří).

Principy:

Paketové filtry

Nejjednodušší a nejstarší forma firewallování, která spočívá v tom, že pravidla přesně uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket, tj. kontrola se provádí na třetí a čtvrté vrstvě ISO OSI.

Stavová inspekce (statefull inspection)

Mnohé útoky lze dnes rozpoznat až tehdy, když si firewally začínají všímat také vzájemných souvislostí a vztahů, a dokáží si dát "dvě a dvě dohromady". Například když si dokáží uvědomit, že najednou přichází výrazně vyšší množství individuálních požadavků než je obvyklé, což vyvolává náhlé zahlcení toho, kdo má tyto požadavky vyřizovat.

Aplikační inteligence

Firewally - se mohou nejodpovědněji (nejspolehlivěji) rozhodnout, pokud "vidí" až na aplikační vrstvu a detailně rozumí tomu, co se zde odehrává, podle jakých pravidel atd. Bez této schopnosti jsou firewally bezbranné vůči celé řadě "moderních" a čím dál tím častějších útoků, jakými jsou například útoky červů (např. Slammer, Code Red či Nimda), útoky pomocí skriptů (cross-site

scripting), vůči emailovému bombardování (mail bombing) atd. Schopnost dívat se až na úroveň aplikační vrstvy je samozřejmě nesmírně náročná na inteligenci firewallu, i na jeho výpočetní kapacitu a správu.

IDS

Nejnověji se do firewallů integrují tzv. in-line IDS (Intrusion Detection Systems – systémy pro detekci útoků). Tyto systémy pracují podobně jako antiviry a pomocí databáze signatur a heuristické analýzy jsou schopny odhalit vzorce útoků i ve zdánlivě nesouvisejících pokusech o spojení, např. skenování adresního rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod.

Ověřit si zabezpečení a popř. funkčnost firewallu je možné. Při online testech se však bude testovat váš počítač pouze máte-li veřejnou IP adresu.

netstat –abn
http://www.paranoia.cz/test/start
http://www.test.bezpecnosti.cz/

Některé SW produkty

FIREWALLY:

Sunbelt Kerio Personal Firewall (zdarma pro domácí nekomerční použití)

ZoneAlarm (zdarma pro osobní a nekomerční použití)

Comodo Firewall (aktivace zdarma, zdarma celoživotní licence)

Symantec Norton Internet Security / Personal Firewall

Agnitum Outpost Firewall Pro

Internet Security Systems BlackICE PC Protection

a další…

(http://www.matousec.com/projects/windows-personal-firewall-analysis/links.php)