

BEZPEČNOST PC DOMA

Jméno: Vladimír Kudělka
Třída: 7.AK
Datum: 18.11. 2003

Vlastní pohled na nebezpečí

Dodnes jsem se tímto tématem (bezpečností) vlastně ani moc nezabýval a vždy zabezpečení domácího PC tak nějak nedbale přecházel. Jako běžný uživatel sice nejsem pod žádným tlakem a moje PC není plné důležitých dat, ale na druhou stranu stále přibývá dotěrných hackerů a také spywaru a při troše štěstí vám mohou vzniknout i větší škody.

Navíc mám já sám s touto problematikou silně nulové zkušenosti, takže v následujících řádcích se budou vyskytovat moje nové zkušenosti, které budou hraničit s prvními poznatky a budu se zabývat nejrozšířenější problematikou.

Spyware

Spyware je udělán tak, že při instalaci daného programu, se spolu s ním nainstaluje malá utilitka, která s programem nijakým způsobem nespojuje, a ta pak posílá informace o vás, vašich heslech a další údaje stažené z vašeho počítače firmě, která tuto utilitku vytvořila.

Schopnosti zjištění přes Spyware

- Vaše systémové jméno uvedené v systémovém registru
- Vaši IP adresu - tj. adresu vašeho počítače po připojení na internet
- Reverzní záznam DNS adresy (dává informaci o tom, k jakému poskytovateli připojení využíváte, a v jakém státě se nacházíte)
- Seznam všech nainstalovaných programů, které mají záznam v systémovém registru (a to nejen záznamy firem, se kterými je spyware produkt distribuován)
- Seznam reklam, které jste otevřeli
- Všechny záznamy o stahování souborů z internetu
- Údaje o souborech uložených na vašem počítači: název, velikost, datum a čas vytvoření souborů, typ souborů
- Záznamy o aktivitě na internetu, tj. kdy jste byli na jaké adrese
- Pokud jste připojeni pomocí vytáčené telefonní linky, telefonní čísla, kam se připojujete
- Heslo pro připojení k internetu pomocí dial-up'u, jestliže jste použili možnost "pamatovat heslo"
- Každé otevření multimediálního souboru

Využití spywaru v praxi

Proč to všechno výrobci implementují do svého software? Nikoli proto, aby mohli nějakého člověka sledovat, co právě s počítačem dělá, nebo aby si mohli číst vaši korespondenci. Všechno se točí kolem marketingu a takto získané statistické informace jsou totiž velmi cenné. Odborník z nich dokáže vyčíst mnoho věcí. Používají se hlavně jako pomůcka při vývoji software. Například se takto dá vysledovat, jaké funkce programu uživatelé používají častěji a jaké ne. Podle toho programátoři onu funkci budou více rozvíjet, nebo ji naopak třeba z programu vypustit. Také se tyto informace používají k lepšímu cílení reklamy.

O spyware se nedá říci, že je špatné. Pomáhá to marketingu. Oztrátě soukromí se také nedá mluvit v obrovských anonymních databázích o něj nepřejdeme. Současně se však také nedá předpokládat, že všechny programy tohoto typu jsou bezpečné. Dá se také čekat, že se s tímto typem programů budeme setkávat čím dál tím častěji.

Prevence

Jako prevence existuje mnoho kvalitních programů. Za zmínku stojí například:

SpywareBlaster, který zabraňuje instalaci nežádoucích špionážních programů, jakými jsou GAIN, Gator, CyDoo, Alexa či Loop, na pevný disk počítače. V databázi programu si můžete nastavit, před

jakými škodlivými objekty z webových stránek má PC chránit. Samozřejmostí je pak záloha nastavení PC, pro pozdější použití při infekci agenty.

Adware Agent chrání před více než 320 Active-X prvky, které se instalují do Internet Exploreru. Dále ochrání počítač před více než 30 tzv. pomocníky, lištami, které se tváří jako pomocníci. Avšak většinou se jedná o spyware.

Hacking

Využití Firewallů

Jako primární zabezpečení proti vnikům nežádoucích osob do vašeho PC můžeme považovat firewall. Ten však určitě neposkytne 100% ochranu. Bezpečnost sítě je komplexní problém a řešení sestává z více komponent – firewall, antivir, VPN, IDS, URL filter, autentikace atd. Firewall je tedy zařízení, které slouží pro fyzické oddělení privátní sítě od Internetu. Firewall pak plní funkci dohledu nad veškerou komunikací mezi vaší LAN a internetem. Běžným příkladem použití je ochrana firemní sítě proti nepovoleným přístupům z internetu. Firewally se dělí do tří základních skupin:

1. Paketové filtry – Packet Filters

- Jsou často implementovány na routerech.
- Vyznačují se vysokou rychlostí, avšak nízkou úrovní zabezpečení, protože kontrolují pouze zdrojovou a cílovou adresu a port.
- Neumožňují logování událostí a nejsou ani schopné upozornit administrátora na podezřelé aktivity.

2. Aplikační brány – Applications Gateway or Proxies

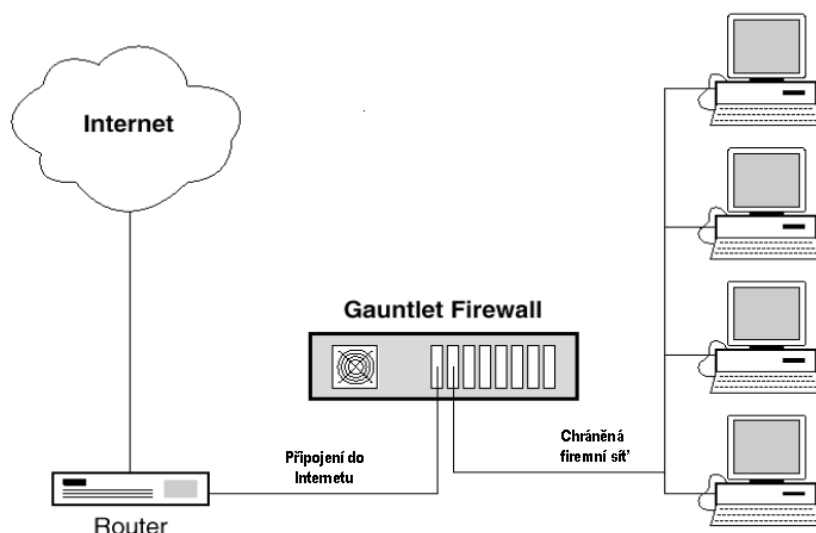
- Jsou podstatně bezpečnější než paketové filtry, ale na druhou stranu jsou pomalejší a omezují uživatele na úzce vymezený okruh služeb (běžně 3 až 7), které jsou podporovány.
- Pro každou další službu je zpravidla nutné napsat nový tzv. proxy, neboli aplikaci, která se postaví mezi chráněnou a nedůvěryhodnou síť a kontroluje všechny pakety pro danou službu.
- Navíc, protože proxies pracují v aplikační vrstvě OSI modelu, nijak nechrání před případným útokem samotný počítač, na kterém běží.

3. SMLI - Stateful Multi-Layer Inspection Gateways

V sobě zahrnují to nejlepší z obou předchozích skupin: rychlost paketových filtrů a zároveň zabezpečení na stejné (nebo lepší) úrovni, jako aplikační brány

Souhrnem se jedná o první obrannou linii. Jeho úkolem je zakázat podle definovaných pravidel veškerý nechtěný provoz. Firewall řídí přístup, dále pak ověřuje uživatele, často funguje i jako VPN gateway a poskytuje i ochranu před útokem typu odepření služby (DoS – DenialofService). Statefullinspectionfirewall pracuje na 3. a 4. vrstvě. Firewall typu applicationlevelgateway pracuje na 7. vrstvě, ale s omezením jen pro několik málo aplikací. Řada hackerských útoků se odehrává na aplikační vrstvě a používá techniky, které firewall nedokáže odhalit. To je úkolem IDS – IntrusionDetectionSystem, který představuje druhou obrannou linii.

Segmentu menších společností se nevyplatí pořizovat vlastní kvalitní firewall pro ochranu lokální sítě právě z důvodu vysokých investic. Cenově efektivní volbou zabezpečení je ochrana pomocí tzv. sdíleného firewallu. Základní princip služby spočívá v tom, že veškerá firemní komunikace odchází od uživatele šifrovaným tunelem na firewall poskytovatele zajišťující ochranu firemního systému. Veškerá zařízení a software jsou ve vlastnictví a v prostorách poskytovatele a uživatel sdílí firewall poskytovatele spolu s dalšími uživateli.



Jako v případě spyware, existuje i v této oblasti mnoho kvalitních programů. Zde je uvedeno pár příkladů:

Outpost Firewall je další z řady osobních firewallů, který si již získal mnoho příznivců. Ochrání vás před hackery, zabrání úniku informací z vašeho počítače, neustále monitoruje síťovou aktivitu, atd.

Sygate Personal Firewall je obranný systém pro malé sítě pracující ve dvou směrech. Jednak se snaží zabezpečit ochranu proti průniku zvenku (tedy z Internetu) a na druhé straně zabraňuje neoprávněné komunikaci jiných softwarových produktů, které zasílají data z Vašeho počítače Ven do internetu. Obvykle se tyto programy, které svým konáním nejen blokují připojení, ale hlavně mnohdy zasílají osobní údaje o uživateli, sdružují pod pojmem Spyware. Ochrana proti útokům zvenku je realizována na podobném principu jako u Proxy serverů.

Amor2net nabízí kromě ochrany před nežádoucí komunikací počítače s Internetem ještě blokování popup oken a odstraňování spywaru. Lze nastavit pravidla jak pro jednotlivé aplikace tak pro celý počítač jako takový. Aktuální připojení je možno sledovat na přehledném výpisu a kterékoli z nich zrušit, pokud je to třeba. Stejně tak lze zapnout i zámek pro veškerou komunikaci s vnější sítí. Program se příliš nehodí pro počítače zapojené do místní sítě (LAN), ale pro zajištění jednoho počítače doma nabízí poměrně dobré řešení, které určitě stojí za vyzkoušení.

Závěr

V tomto projektu jsem shrnul možnosti prevence, proti neoprávněným vniknutím do mého PC. Doposud mě však tato činnost nějak výrazně nepoškodila, ale v budoucnu je to samozřejmě možné. Určitě bych se na tuto problematiku díval z jiného úhlu, kdyby se nejednalo o moje domácí PC, ale byl bych například majitelem firmy a chránil svá důležitá firemní data. V takové oblasti mohou vzniknout opravdu nenahraditelné škody.

Použité zdroje:

Internet:

www.contactel.cz
www.globalnet.cz
www.skynet.cz