МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КРАСНОДОНСЬКИЙ ПРОМИСЛОВО ЕКОНОМІЧНИЙ КОЛЕДЖ

Реферат

з предмету: «Інформаційна безпека»

На тему: «Сильніше загроза - міцніше захист»

Студента групи 1ОКІСМ-06

Петренко Михайла

Перевірила: Дрокіна Т. М.

Краснодон

2009

Зовнішній периметр: міжмережеві екрани

Першу лінію захисту від хакерів, інтернет-черв'яків, програм-шпигунів і інших ворогів тримає міжмережевий екран.

У багатьох компаніях, і навіть у деяких домашніх мережах доступ до інтернету здійснюється через загальне широкосмугове з'єднання. Для того щоб з'ясувати рівень захисту, який забезпечується апаратними міжмережевим екранами, ми протестували дві моделі маршрутизаторів з вбудованими точками доступу: Linksys Wireless-G Broadband Router WRT54G і Microsoft Wireless-G Base Station MN-700. До складу цих маршрутизаторів як побічного продукту для обробки інтернет-трафіку входить найпростіший міжмережевий екран.



Використовуючи трансляцію мережевих адрес (Network Address Translation, NAT) і протокол динамічної конфігурації хоста (Dynamic Host Configuration Protocol, DHCP), маршрутизатор розподіляє серед комп'ютерів мережі приватні IP-адреси, приховуючи їх таким чином від зовнішніх комп'ютерів, які "бачать" тільки IP - адресу самого маршрутизатора. Маршрутизатор відкриває інтернет-порти тільки в тому випадку, якщо його так налаштувати, або якщо комп'ютер мережі запрошує дані з інтернету (наприклад, звертається до веб-сторінці).

Маршрутизатори перешкоджають атакам, при яких хакери використовують засоби сканування портів для пошуку вразливих об'єктів. Якщо жодна із систем мережі не запрошувала пакети даних, маршрутизатор просто відкидає вхідні пакети. Обидва продукти дозволяють відкрити певні порти і призначити їм IP-адреси призначених для цього комп'ютерів. Цей процес, відомий як пересилання порту (port forwarding), дозволяє виділити окремі сервери для ігор в онлайні і відвідування веб-сайтів, не відкриваючи доступ до інших комп'ютерів мережі. У модулі від Microsoft є ще одна приємна функція: за замовчуванням у ньому включено WEP-шифрування; для захисту бездротового трафіку генерується спеціальний ключ.

Комп'ютер під захистом програмного брандмауера

Маршрутизатор захищає від атак ззовні. Проте деякі типи зловмисного програмного забезпечення, такі як інтернет-черв'яки, троянські програми і програми-шпигуни, працюють зсередини. Для того, щоб припинити їх діяльність, необхідний програмний захисний екран, встановлений безпосередньо на комп'ютері.

Брандмауер, налаштований виключно за принципом повноважень доступу, попереджає про будь-якій спробі програми передати дані по мережі і дозволяє блокувати цю операцію, таким чином звертаючи увагу адміністратора на додатки, які можуть виявитися зловмисними.

З міркувань зручності міжмережеві екрани, вбудовані в пакети Panda Platinum Internet Security і Symantec Norton Internet Security 2004 автоматично надають повноваження багатьом додаткам Windows. Проте такий крок може призвести до порушення захисту. Наприклад, спочатку продукт Panda, надаючи доступ служб Windows, залишав відкритим порт 135 - саме через цей порт у комп'ютер проникає сумно відомий черв'як Blaster. Щоправда, коли це було відмічено, помилка була виправлена.

Зустрічається і зворотний "перегин": здавалося б, пакет забезпечення безпеки не може блокувати все підряд - він повинен залишити можливість роботи хоча б для власних компонентів. Однак, виявилося, що в McAfee Internet Security Suite 6 це не так. Наприклад, при спробі відправити лист по електронній пошті програма видає повідомлення про те, що MCSHIELD.EXE і MGHTML.EXE (два компоненти пакета McAfee) намагаються отримати доступ до захищеного файлу - тобто до dat-файлу поштового клієнта.

Боротьба з черв'яками

Sygate Personal Firewall Pro 5.5 і Zone Lab ZoneAlarm Pro 4.5 ніколи не були помічені ні в атаці на "своїх, щоб чужі боялися", ні у надмірному потуранні по відношенню до інших додатків. Завдяки цьому вони надають широкі можливості контролю за системою. Однак якщо нетерплячий адміністратор буде спочатку тиснути на кнопку OK, а потім думати, про що ж це його попереджають, то він поставить систему великому ризику.

Візьмемо, наприклад, черв'як Bagle, який маскується під Windows Explorer. Коли він намагається передати дані в інтернет, міжмережеві екрани McAfee, Norton, Sygate і ZoneAlarm фіксують це і дають адміністратору відповідний запит. Якщо той проявить досить пильності, то зацікавиться, навіщо це Провіднику раптом знадобилося вийти в Мережу. Але якщо адміністратор "проспить" тривожний сигнал і просто натисне OK, то буде сам відповідати за наслідки.

Щоб уникнути подібних проблем можна скористатися міжмережевим екраном з фільтрацією портів (екран такого типу вбудований в Windows XP) або з фільтрацією портів і пакетів, як у Trend Micro PC-cillin Internet Security 2004. При фільтрації пакетів міжмережевий екран контролює передача в обох напрямках між мережею та комп'ютером, на предмет відомих уразливих місць або підозрілої поведінки. Наприклад, таким чином блокуються спроби "нелегального" доступу до портів, що відкривається поштовими вірусами-хробаками, для отримання інструкцій від віддаленого хакера.

Взагалі-то в обов'язки брандмауера не входить "вилов" хробаків і нелегальних програм - це справа антивіруса. Однак антивірусні сканери краще всього працюють тоді, коли можуть порівняти потенційний вірус з базою даних вже відомих вірусів. Якщо ж вірус "свіжий", то він часто залишається нерозпізнаним до тих пір, поки не буде внесено в базу даних і поки вона не буде поновлена на зараженому комп'ютері. На це може піти від кількох годин до декількох днів, а з урахуванням ліні адміністратора - і тижнів.

Проведені тести показали наступні можливості поширених міжмережевих екранів. При спробі програми організувати масову поштове розсилання, що містить її копії, McAfee і ZoneAlarm блокують цю операцію незалежно від того, чи розсилаються листи все відразу або по черзі, при цьому користувач отримує попередження. Panda зупиняє "хробака" інакше: блокує всі вихідні листи, що містять у вкладеннях виконувані файли.

Якщо ж черв'як, такий як Bagle, намагається нелегально відкрити порт системи та отримає інструкції від віддаленого хакера, Panda нічого не може зробити. Маршрутизатори ж блокують цю дію, а програмні міжмережеві екрани, работающіепо принципом надання повноважень, - McAfee, Norton, Sygate і ZoneAlarm - попереджають про нього користувача. Втім, при цьому вони беруть хробака за Windows Explorer, не повідомляючи, що насправді це черв'як, що маскуються під Провідник. Міжмережеві екрани з фільтрацією портів PC-cillin і екран Windows XP захищають комп'ютер тихо і надійно - вони самі блокують спроби хробака отримати доступ до порту, не змушуючи користувача гадати над значенням попереджень.

Зловмисні програми не тільки по-тихому відкривають порти - вони можуть начисто "оголити" комп'ютер, відключивши систему захисту. Panda, Sygate і ZoneAlarm чинять опір таким атакам, але міжмережевий екран Windows XP, McAfee, Norton та Trend Micro вимикаються під впливом коду вторгнення - більше того, такий код здатний видалити файли останніх трьох пакетів.

Об'єднаними силами

Маршрутизатори, такі як моделі Linksys і Microsoft, відображають зовнішні атаки, в той час як програмні міжмережеві екрани захищають комп'ютерні системи від вірусів-хробаків, що поширюються через диски загального доступу, електронну пошту і додатки для обміну файлами, такі як Kazaa і Gnutella. Програмні міжмережеві екрани - необхідний захисний компонент для ноутбуків, що підключаються не тільки до захищеної офісної або домашньої мережі, а також до мереж загального доступу, особливо бездротовим.

З розглянутих міжмережевих екранів нам найбільше сподобалися Sygate і ZoneAlarm. Sygate впачатляет швидкодією і модульної конфігурацією, завдяки якій його можна налаштовувати практично як завгодно. Щоправда, деякі його повідомлення здатні поставити в глухий кут, незважаючи на деталь. Як, наприклад, реагувати на таке попередження: "Internet Explorer (IEXPLORE.EXE) is trying to connect to (207.46.134.221) using remote port 80 (HTTP - World Wide Web)"? Навіть у перекладі на російську - "Internet Explorer (IEXPLORE.EXE) намагається з'єднатися з www.microsoft.com (207.46.134.221) через віддалений порт 80 (HTTP - World Wide Web)" не зовсім зрозуміло ... А ось повідомлення ZoneAlarm в тій же ситуації цілком ясно: "Do you want to allow Internet Explorer to access the Internet?" - "Чи дозволяєте ви доступ Internet Explorer до інтернету?".

Швидкодія ZoneAlarm не гірше, ніж у Sygate, а інтерфейс значно зрозуміліше. Тим же, кому не вистачає терпіння настроювати міжмережевий екран, що працює за принципом надання повноважень, можна порекомендувати екран з фільтрацією портів, такий як PC-cillin.

Внутрішня безпека: антивіруси

Незважаючи на те, що міжмережеві екрани успішно блокують ряд вірусів, зондувальних мережеві порти, і затримують деякі спроби їх масового саморозмноження по електронній пошті, в системі все одно необхідний антивірусний сканер, який би зупиняв більшість інфекцій, що потрапляють у комп'ютер через електронну пошту та файли, скачувати з Інтернету. Знешкоджувати цю інфекцію може тільки антивірусний сканер. Крім сканерів, що входять до складу описаних вище пакетів по забезпеченню безпеки, ми розглянули два самостійних продукту: Grisoft AVG Anti-Virus Professional і Eset NOD32 2.

Всі ці продукти відповідають мінімальним вимогам по "вилову" основних зловмисних програм, що зустрічаються в інтернеті - тих, що хоча б двічі згадуються членами WildList Organization (www.wildlist.com), всесвітнім суспільством розробників антивірусних програм. Адже далеко не кожним вірусом справді можна заразитися через Мережу: з приблизно 100000 існуючих вірусів в даний час всього близько 250 зустрічаються в "дикому" інтернеті; інші існують тільки в "лабораторних" умовах. Виявилося, що якість роботи різних сканерів відчутно залежить від типу вірусів. Наприклад, всі відібрані для огляду продукти добре справляються з вірусами і черв'яками, що діють в 32-розрядної середовищі Windows - найбільш поширеним сьогодні типом мережевий "інфекції". В цьому випадку якість розпізнавання дуже високо - від 90,4 до 100%

Однак з троянськими програмами, які поширюються не самі по собі, а за допомогою інших програм, у тому числі вірусів та "хробаків", справа йде гірше: якщо сканери McAfee і Norton затримують відповідно 99% і 95% "троянців", то AVG - всього 23,5%, що навряд чи можна вважати достатнім захистом. Крім того, троянські програми не включаються в список WildList, через що за ними важче стежити. Нарешті, дуже бажано, щоб антивірусний сканер не піднімав помилкову тривогу, підозрюючи в наявності вірусу звичайні файли. У цьому сенсі найкраще йдуть справи у PC-cillin, де тест пройшов без помилкових спрацьовувань; на іншому кінці шкали - Eset NOD32 2, з 32 з 20000 файлів. Звичайно, це настільки мало, що навіть не варто перераховувати у відсотках, а й одного такого випадку достатньо, якщо в результаті замість вірусу буде видалено потрібний файл.

Що робити з новими "мікробами"?

У своїй роботі антивірусні сканери спираються в основному на точну відповідність відомим зловмисних програм, сигнатури яких зберігаються в базі даних. Втім, іноді вони "ловлять" і нові віруси, яких а базі немає, використовуючи евристичні алгоритми. Строго кажучи, слово "евристичний" тут означає можливість ідентифікувати невідомий вірус на підставі якихось характерних ознак - наприклад, коду, що використовує відому "діру" в операційній системі або додатку. На практиці в евристичних алгоритмах пошуку вірусів використовуються різні "нечіткі" схеми розпізнавання нових модифікацій вже відомих вірусів з використанням їх спільних ознак - наприклад, знаючи ознаки вірусу Netsky.gen, можна "відловити" його нові варіанти на зразок Netsky.R.

За даними тестів, з розглянутих програм найбільш вдалими евристичний алгоритм володіють McAfee і AVG, що ідентифікують 70,1% і 65,6% файлів, заражених невідомими вірусами; найгірший результат виявився у NOD32 - 41,4%. І в будь-якому випадку, це набагато менше і повільніше, ніж при розпізнаванні відомих вірусів, тому що основним засобом своєчасного лікування, як і раніше залишається регулярне оновлення антивірусних баз.

Всі програми тестувалися в режимі максимально ретельного сканування. Особливий випадок був NOD32: у цій програмі передбачений підвищений у порівнянні з жорстким диском рівень евристичного сканування Advanced Heuristics для електронної пошти та веб-трафіку, цих основних джерел інфекцій. Для сканування жорсткого диска цей режим теж можна використовувати, але не засобами графічного інтерфейсу, а за допомогою недокументовані команди nod32.exe / AH. У режимі Advanced Heuristics якість сканування NOD32 зростає до 53,5%.

На жаль, всі розглянуті антивіруси успішно розпізнають нові інфекції тільки в тому випадку, якщо останні належать до вже відомих на вірусний "домами", але виявляються безсилі при зустрічі з абсолютно новим вірусом. Наприклад, жоден з сканерів не розпізнав хробака Netsky, поки його сигнатура не була внесена до бази даних.

Таким чином, евристичне розпізнавання вірусів, як і раніше ненадійно. Доводиться спиратися на інші рівні захисту, такі як міжмережеві екрани і власний здоровий глузд.

Найбільш зручний сканер

Якби головним в антивірусному сканері було зручність інтерфейсу, то кращим пакетом напевно був би визнаний McAfee. Правда, в іншому у McAfee багато недоліків - наприклад, помилки в сценарії оновлення, в результаті яких програма повідомляє, що сканер вже був оновлений, у той час як насправді це не так.

McAfee, звичайно, не єдиний пакет з "глюками" - хоча їх у нього й багато. Жодна з розглянутих програм не пройшла гладко тест на видалення вірусу CTX, "троянського коня" Optix і хробака Mydoom.A. Найкраще впорався з очищенням комп'ютера PC-cillin - інфекція була повністю знято, а система не пошкоджена. Після спроб McAfee, NOD32 й Panda видалити CTX (безуспішно) система прийшла в непридатність.

Найбільшим недоліком пакету Norton виявилася його повільність. Коли в системі встановлений цей пакет, вона запускається і відключається удвічі повільніше, ніж при використанні Panda або NOD32, вплив яких на швидкодію найменш помітно. Norton повільніше всіх виконує повне сканування жорсткого диска - перевірка диска зі швидкістю обертання 5400 об / хв, дані на якому займають 575 Мб, на комп'ютері з Windows XP, Pentium III 800 МГцб 256 Мб RAM, триває близько 12 хв. Найшвидша з програм огляду, NOD32, виконує цю операцію всього за 52 с. (Щоправда, Norton краще розпізнає віруси.) Наступним за швидкістю після NOD32 був сканер Panda, впорався із завданням трохи більше ніж за 2,5 хв.

Кращим антивірусом огляду був визнаний пакет Trend Micro PC-cillin Internet Security 2004: ця програма відрізняється не тільки якісним скануванням і розумною ціною, але також логічним і зрозумілим інтерфейсом.

Заповнюючи прогалини: програми-антишпигуни

Безперечно, міжмережеві екрани і антивірусні сканери відіграють значну роль у захисті комп'ютерної системи. Однак іноді вони пропускають програми, породжені специфічними попитом, а саме програми-шпигуни. Втім, до цієї категорії входять не тільки звичайні сканери мишки і клавіатури, а й, наприклад, "викрадачі браузера" - рід adware (програм для розповсюдження реклами), завданням якого є зміна записів системного реєстру без відома користувача так, щоб замість звернення до домашньої сторінці або стандартного пошукового сервера (наприклад, при помилковому введенні URL) браузер переходив на сторінку з рекламною інформацією.

Багато такі "викрадачів", звані також програмами примусової завантаження, використовуючи недостатню захист системи, часто самоінсталліруются при відвідуванні веб-сторінки. Наприклад, сумно відома утиліта Surfbar (вона ж Junkbar і Pornbar) використовує той факт, що Internet Explorer допускає завантаження виконуваних файлів на комп'ютер користувача. Потім вона заміняє початкову сторінку браузера на www.surferbar.com, завалює робочий стіл сотнею-другий посилань на порносайти і встановлює панель з ще кількома десятками посилань того ж роду. Інші програми-"викрадачів" питають дозволу на початок роботи, але в такий спосіб, щоб обманом змусити користувача погодитися.

Чисті" програми-шпигуни простежують використання інтернету - здебільшого для того, щоб визначити, які що користувач робить в онлайні, і запропонувати йому відповідну рекламу. Як правило, програми-шпигуни супроводжують умовно-безкоштовні та безкоштовні програми. Часто справжня вартість таких "безкоштовних" програм прихована в їх ліцензійній угоді: не читаючи його, користувач погоджується на віддалений моніторинг свого комп'ютера службами, які збирають маркетингові дані або розсилати спрямовану рекламу. Різні країни зараз розробляють закони проти такої діяльності, проте поки що найкращим захистом є сканери-антишпигуни.

Ми досліджували п'ять спеціальних "антішпіонскіх" пакетів:

Auria Spyware Eliminator,

InterMute SpySubtract Pro 2,

Lavasoft Ad-aware 6 Plus,

Network Associates McAfee AntiSpyware,

Spybot Search & Destroy.

Також були розглянуті можливості по "вилову" програм-шпигунів за допомогою антивірусних сканерів і інших утиліт, що входять до складу таких пакетів:

Network Associates McAfee Internet Security Suite 6,

Panda Platinum Internet Security 3,

Symantec Norton Internet Security 2004,

Trend Micro PC-cillin Internet Security 2004.

На жаль, навіть найкращі з них розпізнають ледь більше половини з усіх запропонованих ним зразків шпигунських утиліт. В даний час найкращою стратегією є використання відразу декількох сканерів.

Сканер Norton ідентифікував лише два із запропонованих семи шпигунських утиліт, PC-cillin і Panda - по одній. При установці антивірусів на вже інфікований комп'ютер був виявлений виконуваний файл, яка породжувала інфекцію Surfbar, але видалити вже встановлену панель посилань і піктограми порносайтів, а також повернути на місце первісну домашню сторінку не вдалося. Утиліта McAfee Privacy Service точно розпізнає спроби змінити реєстр і настійно радить користувачеві не піддаватися на провокації, але не виявляє в оперативній пам'яті процеси, які породжують ці дії. Таким чином, не встигне користувач відбити одну атаку, як накочує наступна, і його життя перетворюється на суцільну низку попереджень і відмов, до тих пір, поки він нарешті не вирішить, що краще один раз інфікувати комп'ютер, ніж постійно відриватися від справ.

На відміну від антивірусів, що виявляють інфіковані шляхом порівняння їх з сигнатурами зловмисних програм з бази даних, антишпигунські сканери спираються головним чином на ключі системного реєстру. Найбільш надійні результати в тестах показали Spybot Search & Destroy і Lavasoft Ad-aware 6 Plus, але Spybot краще видаляв пошкоджені файли і відновлював значення реєстру.

Сканер McAfee AntiSpyware виявив три з семи інфекцій - Gator, Huntbar і MyFast Access, - але повністю видалити зміг тільки дві останні. Слабкіше всіх виявився InterMute SpySubtract Pro 2, який знайшов тільки один зразок програми-шпигуна - широко відому панель Gator.

Хорошу захист у реальному часі забезпечує компонент Ad-watch з Lavasoft Ad-aware 6 Plus. Він перекривав шлях всім "викрадачам браузерів", які намагалися змінити параметри доступу до інтернету. (Щоправда, Ad-watch не входить до розповсюджується безкоштовно спрощену версію Ad-aware.)

На жаль, як з'ясувалося, ні один з протестованих сканерів не забезпечує 100-процентного розпізнавання і видалення інфекції. Найкраще справляються із завданням Spybot Search & Destroy і Lavasoft Ad-aware 6 Plus. У Ad-aware краще організований моніторинг шпигунських утиліт і зручніше інтерфейс, зате Search & Destroy краще знаходить і чистить інфіковані файли.

Висновки

В ідеальному випадку захист від нападів з інтернету не повинна бути багаторівневою. У майже ідеальному випадку можна було б обійтися одним пакетом із забезпечення безпеки або хоча б комплектом програм одного виробника. На жаль, жоден з протестованих пакетів не закриває усі вразливі місця досить надійно. Зокрема, жоден з них не забезпечує надійне виявлення і видалення шпигунських програм.

В цілому, кращим з розглянутих пакетів можна визнати Trend Micro PC-cillin Internet Security 2004 - за кращий антивірусний сканер і один з кращих міжмережевих екранів. У комбінації з безкоштовним Spybot Search & Destroy він забезпечив би достатню безпеку. Для посилення захисту від шпигунських програм можна скористатися Lavasoft Ad-aware 6 Plus (усі три програми добре поєднуються один з одним і працюють без конфліктів). Можливостей брандмауера PC-cillin повинно бути достатньо для більшості користувачів. Якщо ж захочеться чогось міцніше, можна відключити міжмережевий екран PC-cillin і встановити Zone Labs ZoneAlarm Pro 4.5 (наприклад, спрощену безкоштовну версію).

На жаль, жоден з розглянутих пакетів не містить по-справжньому надійної утиліти по боротьбі зі спамом. Для цього доводиться встановлювати додаткові продукти.

Ешелонована оборона

Багаторівнева система, що затримує атаки і забезпечує своєчасне резервне копіювання даних, складається з наступних рівнів.

Апаратний маршрутизатор:

за допомогою NAT (Network address Translation, трансляція мережевих адрес, - стандарт Internet, що дозволяє використовувати в локальній мережі різні набори IP-адрес для зовнішнього і внутрішнього трафіку) маскує IP-адреси, роблячи неефективним сканування портів.

блокує надходження даних з інтернету, на які немає дозволу користувача;

не захищає систему від більшості зловмисних програм, таких як "троянські коні", віруси, поштові "черв'яки" і шпигунські програми.

Програмний маршрутизатор:

запобігає несанкціоновану передачу даних з комп'ютера до мережі інтернет "троянцями" та іншими додатками, встановленими без відома користувача;

захищає портативні ПК при роботі в бездротових та інших малозахищених мережах;

блокує деякі зловмисні програми, але не в змозі їх видалити.

Антиспамерські програмне забезпечення:

блокує що вводять в оману, шахрайські ( "рибальські") схеми;

скорочує роботу з фільтрування листів, зменшуючи ймовірність того, що користувач випадково поспіхом активує вірус, отриманий по електронній пошті.

Антивірусне програмне забезпечення:

захищає систему від відомих вірусів, хробаків і "троянців", але менш ефективна проти нових інфекцій;

не захищає систему від програм поширення реклами (adware), шпигунських програм і "викрадачів браузерів".

Антішпіонское програмне забезпечення:

захищає від програм класу adware, шпигунських програм і "викрадачів браузерів", cookies-сканерів і інших інтернет-паразитів.