УДК 004.056(045)

С.В. Єгоров, асист.

ЗАХИСТ ОПЕРАЦІЙНИХ СИСТЕМ ВІД МОЖЛИВИХ ЗАГРОЗ

Національний авіаційний університет
E-mail:sehorov@gmail.com

Розроблено рекомендації для організації безпечного середовища роботи в операційних системах та захисту операційних систем за допомогою антивірусних програм і брандмауерів.

Ключові слова: віртуальні машини, захищений режим роботи операційних систем, операційні системи, рекомендації до захисту операційних систем.

Постановка проблеми

У зв'язку інтенсивним розвитком інформаційних технології (ІТ) на перший план у сучасному суспільстві вийшли інформаційні війни й забезпечення безпеки систем, побудованих на основі ІТ, для ефективного запобігання крадіжки особистої інформації кіберзлочинцями.

Вирішальну роль при реалізації комплексної системи захисту ІТ-систем має реалізація захисту комп'ютерів, які є частиною такої системи (хост-бастіони, брандмауери).

Аналіз публікацій

Багато публікацій присвячено проблемі забезпечення безпеки ІТ-систем, але в них не розкрито повно проблему захисту комп'ютерів, з якими працює кінцевий користувач.

У роботі [1] наведено види загроз, які здатний виявити kis 6.0, але не описано, як використовувати можливості самої операційної системи (ОС) для підвищення ефективності захисту комп'ютера.

У роботі [2; 3] показано, як розгортається й настроюється ОС, але немає нічого про забезпечення безпеки цієї ОС під час її експлуатації.

Мета роботи – розроблення рекомендацій, яких слід дотримуватися при експлуатації ОС для забезпечення стабільності й безпеки.

Джерела загроз

Згідно з роботою [1] джерелом загроз інформаційній безпеці може виступати людина або група людей, а також незалежні від діяльності людини прояви. Усі джерела загроз можна розділити на три групи факторів:

– людський;

– технічний;

– стихійний.

Людський фактор – група загроз пов'язана з діями людини, що має санкціонований або несанкціонований доступ до інформації. Загрози цієї групи можна розділити на такі:

– зовнішні, до них стосуються дії кіберзлочинців, хакерів, інтернет-шахраїв, несумлінних партнерів, кримінальних структур;

– внутрішні, до них відносяться навмисні чи випадкові дії персоналу компаній, користувачів домашніх комп'ютерів.

Технічний фактор – група загроз пов'язана з технічними проблемами:

– фізичне й моральне старіння обладнання, що використовується;

– неякісні програмні й апаратні засоби обробки інформації.

Усе це призводить до відмови обладнання й найчастіше до втрати інформації.

Стихійний фактор – група загроз, що не залежать від діяльності людей:

– природні катаклізми;

– стихійні лиха;

– форс-мажорні обставини.

У ході проектування комплексної системи безпеки необхідно враховувати всі перераховані джерела загроз.

Згідно з роботою [1] види загроз бувають такими:

– хробаки (worms);
– віруси (viruses);
– троянські програми (Trojans);
– програми-реклами (adware);
– програми-шпигуни (spyware);
– програми-жарту (jokes);
– програми-маскувальники (rootkit);
– хакерські атаки, фішинг (phishing);
– додзвін на платні Інтернет-ресурси;
– нав'язлива реклама;
– спам (spam);
– інші небезпечні програми.

Вибір операційної системи

Перед розробкою системи безпеки для ОС слід визначити, яку саме ОС необхідно захищати.

Операційні системи бувають із відкритим і закритим вихідним кодом. Останні – це завжди платні комерційні продукти. На ринку ОС найпоширеніші це Linux і Windows.

Linux і інші линуксоподібни ОС порівняно з Windows, якщо не брати до уваги безкоштовність Linux, мають тільки одну перевагу: відкритість вихідного коду. Тому встановлювати Linux слід тільки тоді, коли без знання вихідного коду ОС обійтися не можливо.

Наприклад, для професійних зайнять хостінгом необхідно встановлювати Linux із відкритим вихідним кодом, щоб була можливість оперативно реагувати на нові загрози безпеки для ОС внесенням змін в її вихідний код.

Windows має добре продуманий інтерфейс користувача, набагато більший асортимент програмного забезпечення. Порівняно з Linux у ній легше розібратися, її набагато простіше настроювати, набагато простіше знайти фахівця здатного обслуговувати Windows і, як наслідок, простіше побудувати систему безпеки для ОС Windows.

Захищений режим роботи операційної системи

Захист від хакерських атак і шкідливих програм забезпечують:
– антивірусні програми;
– екрани;
– хост-бастіони;
– брандмауери.

Але перераховані заходи не забезпечують захист від некваліфікованих дій користувача, некоректної роботи нових установлених програм.

Для вирішення цієї проблеми використовують програмне забезпечення, яке повертає ОС до первинного стану після її перезавантаження, наприклад:
– Shadowuser Pro;
– Deep Freeze Standard;
– Disk Write Copy Professional Edition.

Принцип дії цих програм заснований на тому, що користувач задає диски, які необхідно захищати, й програма відслідковує зміни, які вніс користувач на цих дисках.

Для запуску підозрілих або незнайомих програм можна використовувати програму Sandboxie. Принцип її дії полягає в тому, що програмі, яка запускається в середовищі Sandboxie й компонентам, пов'язаним із нею, виділяється віртуальний ізольований адресний простір. Кількість цих просторів обмежується лише ресурсами ОС. До недоліків Sandboxie слід віднести те, що не всі програми здатні запускатися в її середовищі.

Як безпечне робоче середовище можна використовувати й гостьові ОС. Це можна реалізувати, наприклад, за допомогою таких віртуальних машин, як Oracle VM Virtualbox або Microsoft Virtual PC 2007 SP1. Останній продукт підтримує тільки ОС від Microsoft.

На базі таких віртуальних машин можна реалізувати віртуальний хост-бастіон.

В операційній системі від Microsoft реалізована функція тіньового копіювання томів. Вона виконується згідно з розкладом, перед інсталяційними процесами або виконується користувачем вручну. Це дозволяє повернутися до первинного стану ОС, яке було на момент зняття тіньової копії томів. При використанні засобів резервного копіювання, які вбудовані в ОС Windows, необхідно враховувати обмеження, які описані в документації для ОС.

Ефективність використання програм доведено їхнім використанням в інтернет-кафе й навчальних закладах.

Антивірусні програми й брандмауери

Важливе місце в захисті ОС займає захист від шкідливих програм і хакерських атак. Жодна антивірусна програма не може гарантувати виявлення всіх шкідливих програм. Це стосується навіть найвідоміших брендів.

Щорічно кількість шкідливих програм росте в арифметичній прогресії. З величезної кількості вірусів, які з'являються щодня, хробаків антивірусні програми здатні швидко виявити лише дві третини. Навіть на сьогодні зустрічатися «звірки», що з'явилися років п'ять тому, і які не здатна виявити жодна антивірусна програма.

Серед розроблювачів шкідливого програмного забезпечення дуже часто зустрічаються талановиті програмісти, які прикладають максимум зусиль для приховання факту роботи своєї розробки.

Антивірусна програма це всього лише алгоритм, який має безліч обмежень, а штучний інтелект поки ще не створений.

Антивірусна програма не перешкоджає проникненню загроз ззовні, а дозволяє боротися тільки з наслідками зараження ОС.

Завдання брандмауера полягає в створенні фільтрів, які перешкоджають передачі несанкціонованих пакетів в ОС або з неї.

Брандмауер контролює весь мережний трафік, аналізуючи природу й достовірність його походження. Передавання даних при цьому має бути пов'язано з певним додатком і відбуватися за певними правилами:

– протокол;
– порт;
– напрямок передачі;
– походження ініціатора запиту.

Повноцінно захистити ОС можливо, лише контролюючи всі можливі шляхи проникнення в систему.

Недоліком брандмауера є нездатність захистити систему, якщо зараження вже відбулося, наприклад, якщо троян здійснює передачу даних з протоколом HTTP за допомогою веббраузера. Для того щоб перекрити види загроз потрібно комбінувати антивірусну програму з брандмауером. При цьому рекомендується використовувати рішення, в яких поєднані антивірусна програма із брандмауером (Comodo Internet Security, Kaspersky Internet Security).

Для зниження ймовірності проникнення шкідливого програмного забезпечення в ОС можна використовувати той факт, що в сім'ї Microsoft® Windows, починаючи з NT, кожний процес має свій контекст безпеки. Тому є можливість розмежувати права доступу до файлів і програм для різних користувачів на рівні файлової системи.

Висновки

Ефективність використання програм, які повертають ОС до первинного стану після перезавантаження й виділяють ізольоване віртуальне середовище для запуску програмного забезпечення, доведено їх застосуванням в інтернет-кафе й у навчальних закладах. Організація захисту ОС від хакерських атак і шкідливого програмного забезпечення досить важке завдання. Це пов'язане з тим, що протистояти доводиться фахівцям, які мають високу кваліфікацію й інтелект.

Розроблювачі програм захисту не в змозі повністю відслідковувати появи нових шкідливих програм й хакерських атак. Єдиний спосіб протистояти всім видам загроз, які впливають на ОС із закритим вихідним кодом – це відстеження й своєчасна установка відповідних оновлень для ОС, а також своєчасне оновлення антивірусних баз. Дотримуючись усіх викладених рекомендацій, можна значно знизити ймовірність втрати інформації від впливу різних загроз на ОС.

Література

1. *Kaspersky* Internet Security 6.0. [электронный ресурс]: © ЗАО «Лаборатория Касперского» – Электорон. дан. (1 файл). – М., 2007. – 319 с. – Режим доступу: http://docs.kasperskylabs.com/russian/kav6.0ru.pdf. – Назва з екрана.

2. *Microsoft*® Windows 2000 Server. Русская версия / А.Г. Андреев, Е.Ю. Беззубов, М.М. Емельянов и др. – СПб.: БХВ-Петербург, 2003. – 960 с.

3. *Introduction* to Comodo Internet Security [Electronic resource]: © Comodo Group, Inc. – Mode of access: WWW.URL: http://help.comodo.com/ topic-72-1-155-1074-Introduction-to-Comodo-Internet-Security.html. – Title from the screen.

Стаття надійшла до редакції 11.04.2011.