логических функций / С.В. Рудницкий, Р.П. Мельник, В.В. Веретельник // Вектор науки Тольяттинского государственного университета. – 2012. — № 4 (22). — С. 119–122.

3. Миронюк Т.В. Синтез елементарних функцій перестановок, керованих інформацією / Т.В. Миронюк, О.Г. Мельник // ІІ Міжнародна науково-практична конференція «Інформаційні технології в освіті, науці й техніці» (ІТОНТ-2014), 24- 26 квітня: зб. тез. доп. — Черкаси : ЧДТУ, 2014. — С. 147-148

4. Рудницький В. М. Синтез елементарних функцій перестановок, керованих інформацією / В.М. Рудницький, Т. В. Миронюк, О.Г. Мельник, В.П. Щербина // Безпека інформації том 20, №3. – Київ: НАУ, 2014. – С. 242-247

5. Криптографическое кодирование: коллективная монография / Под ред. В.Н. Рудницкого, В.Я. Мильчевича. – Харьков : Изд-во «Щедрая усадьба плюс», 2014. – 240 с.

6. Миронюк Т. В. Визначення елементарних операцій базової групи перестановок керованих інформацією / Т. В. Миронюк // Вісник Черкаського державного технологічного університету. – 2016. – Випуск №2. – С. 100-105.

References

1. Vera Babenko Olga Melnyk Ruslan Melnik.(2013). Classification of three digit basic functions for cryptographic transformation of information // Security of Information, (1(19)), pp. 56-59. (in Ukr.).

2. S.V. Rudnytskyy. (2012). The cryptographic transformation of information based of three digit logical functions / S.V. Rudnytskyy, R.P Melnyk, O. V. Veretelnyk // Vector Science Togliatti state-owned university, (4 (22)), - pp. 119-122.

3. Myronyuk T.V. Synthesis permutations of elementary functions controlled by the information / T.V. Myronyuk, O.H. Melnyk // Conference proceedings of II International Scaintifical-Practical Conference “Information Technologies in Education, Science and Technology” (ITEST-2014): Cherkasy, April 24-26, 2014, - 2 volumes.- Cherkasy: ChSTU, 2014. – pp. 147-148. (in Ukr.).

4. Rudnytskyy V., Melnyk O., Scherbyna V., Myronyuk T. Synthesis of elementary transposition functions controlled by information // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 242-247. (in Ukr.).

5. The cryptographic coding: collective monograph / Ed. V.N. Rudnicki, V.Y. Milchevich. - Kharkov: Publishing house "Schedraya usadba plus", 2014. – 240 pp. (in Rus.)

6. Myronyuk T.V. Definition of elementary operations of core group permutations which is managed by information / T.V. Myronyuk // Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitety. 2016. No. 2. P. 100-105. (Ukr)

АНАЛІЗ ЕФЕКТИВНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП’ЮТЕРНИХ СИСТЕМАХ

Стрембіцький Р.Г.,
магістрант,
Черкаський державний технологічний університет,
Черкаси, Україна

Кобильник О.Б.
магістрант,
Черкаський державний технологічний університет,
Черкаси, Україна

ANALYSIS OF THE EFFECTIVE METHOD OF PROTECTING INFORMATION IN COMPUTER SYSTEMS

Strembitskyi R.G.,
undergraduate,
Cherkassy State Technological University,
Cherkassy, Ukraine

Kobylnyk O.B.,
undergraduate,
Cherkassy State Technological University,
Cherkassy, Ukraine

Анотація

В статті проведено дослідження та аналіз найбільш дієвих методів захисту комп’ютерних систем від несанкціонованого доступу та крадіжки інформації. Такими методами захисту вважаються: міжмережевий екран (Firewall, брандмауер), аркуші доступу (access-lists), NAT (Network Address Translation),

proxy-сервер, антивірусний захист поштової системи та log-сервер. У кожного з приведених методів є свої переваги та недоліки, про які і говориться в статті. Проведений аналіз дозволяє зробити вибір методу захисту інформації відповідно до вимог, які висуваються до комп'ютерної системи, та до параметрів даної системи.

Ключові слова: *Захист інформації, комп'ютерна система, несанкціонований доступ, міжмережевий екран (Firewall, брандмауер), аркуші доступу (access-lists), NAT (Network Address Translation), proxy-сервер, антивірусний захист поштової системи, log-сервер.*

ABSTRACT

In the article conducted the research and analysis of the most effective methods of protecting computer systems from unauthorized access and information theft. These methods of protection are considered a firewall, access-lists, NAT (Network Address Translation), proxy server, email antivirus protection system and log-server. Each of the resulted methods has their advantages and disadvantages, which also said in the article. The analysis allows choosing the method of information security in accordance with the requirements that apply to the computer system and the parameters of the system.

Keywords: *Data protection, computer system, unauthorized access, firewall, access-lists, NAT (Network Address Translation), proxy server, email antivirus protection system, log-server.*

Вступ

Будь-яка система, що підключена до мережі Інтернет, повинна бути захищена. Проблема захисту систем, підключених до мережі Інтернет, є досить актуальною серед користувачів. Існує багато способів захисту системи, але потрібно пам'ятати, що будь-який захист ускладнює використання системи (обмежує можливості деяких функцій, споживає обчислювальні й трудові ресурси, вимагає фінансових витрат на створення та використання системи). Тож, чим надійніший захист, тим більш затратною і менш зручною для користувачів стає система.

Метою статті є дослідження та аналіз найбільш надійних методів, які забезпечать захист і безпеку комп'ютерної системи.

Часткове вирішення проблеми захисту комп'ютерних систем від несанкціонованого доступу через мережу Інтернет можливе за допомогою певних пристроїв та програм. Серед дієвих методів варто згадати міжмережевий екран (Firewall, брандмауер), аркуші доступу (access-lists), NAT (Network Address Translation), proxy-сервер, антивірусний захист поштової системи, log-сервер.

Міжмережевий екран (Firewall, брандмауер)

На думку багатьох експертів з захисту інформації найкращим методом захисту системи є міжмережевий екран (Firewall, брандмауер).

Міжмережеві екрани реалізують набір правил, які визначають умови проходження пакетів даних з однієї частини розподіленої комп'ютерної мережі (відкритої) в іншу (захищену).

Брандмауер установлюється між мережею та Інтернетом і виконує роль мережного фільтра. Він налаштовується таким чином, щоб пропускати допустимий трафік від користувачів мережі до служб Інтернету і назад, та максимально обмежити трафік з боку Інтернету до мережі, яка захищена, тільки необхідними службами, такими як: smtp, dns, ntp. Мережевий адміністратор визначає допустимість того або іншого трафіка. Брандмауер відслідковує кожне мережне з'єднання окремо і контролює весь процес у динаміку. При встановленні нового TCP-сеансу міжмережевий екран створює для нього новий процес, що контролює правильність з'єднання до самого моменту його завершення. Разом з цим кожний пакет на транспортному рівні перевіряється на відповідність попередній, а всі "підозрілі" пакети відкидаються. Це дозволяє організувати фільтр для доступу внутрішнього комп'ютера до зовнішнього, але не дозволяє зовнішньому комп'ютеру самостійно звернутися до внутрішнього. Інакше кажучи, міжмережевий екран задає правила для проходження трафіка від одного інтерфейсу до іншого, для кожного напряму й кожного тракту окремо. Якщо правило дозволяє проходження IP-пакета від інтерфейсу внутрішньої мережі до Інтернет інтерфейсу, то на підставі такого пакета формується логічний тунель у маршрутизаторі, через який уже можуть пройти відповідні пакети від зовнішнього одержувача. Як тільки з'єднання закрите або час очікування вичерпаний, тунель закривається і доступ інформації до внутрішнього комп'ютера стає обмеженим. З цієї ж причини, екран не пропустить пакети у зворотному напрямі, якщо ініціатором з'єднання є зовнішній комп'ютер [1].

Залежно від рівня взаємодії об'єктів мережі Брандмауери поділяються на фільтруючі маршрутизатори, шлюзи сеансового та прикладного рівнів. Фільтруючі маршрутизатори, які працюють на мережному рівні, фільтрують пакети даних, що входять у захищену частину мережі або вихідних з неї.

Переваги фільтруючих маршрутизаторів:

+ простота їх створення;

+ установка і налаштування;

+ мінімальний вплив на продуктивність комп'ютерної мережі;

+ невисока вартість.

Недоліки фільтруючих маршрутизаторів:

- відсутність автентифікації на рівні користувачів комп'ютерної мережі;

- уразливість для підміни IP-адреси в заголовку пакета;

- незахищеність від погроз порушення конфіденційності й цілісності переданої інформації;
- сильна залежність ефективності набору правил фільтрації від рівня знань адміністратора брандмауера конкретних протоколів;
- відкритість IP-адрес комп'ютерів захищеної частини мережі.

Шлюзи сеансового рівня призначені для контролю віртуального з'єднання між робочою станцією захищеної частини мережі й хостом її незахищеної частини і трансляції IP-адрес комп'ютерів захищеної частини мережі. У процесі виконання шлюзом сеансового рівня процедури трансляції IP-адрес відбувається їхнє перетворення в одну IP-адресу, асоційовану із міжмережевого екрану. Це виключає можливість прямої взаємодії між хостами захищеної й відкритої мереж і не дозволяє зловмиснику здійснювати атаку шляхом підміни IP-адрес.

Перевагою шлюзів сеансового рівня є їх простота та надійність програмної реалізації.

Недоліком є відсутність можливості перевіряти вміст переданої інформації.

Шлюзи прикладного рівня не тільки відкидають можливість прямої взаємодії між уповноваженим користувачем із захищеної частини мережі й хостом з її відкритої частини, але й фільтрують усі вхідні й вихідні пакети даних на прикладному рівні.

Основні функції шлюзів прикладного рівня:

- ідентифікація й автентифікація користувача КМ при спробі встановити з'єднання;
- перевірка цілісності переданих даних;
- розмежування доступу до ресурсів захищеної й відкритої частин розподіленої мережі;
- фільтрація і перетворення переданих повідомлень (виявлення шкідливого програмного коду, шифрування й розшифрування та ін.);
- реєстрація подій у спеціальному журналі;
- кешування запитуваних ззовні даних, розміщених на комп'ютерах внутрішньої мережі.

Переваги шлюзів прикладного рівня:

+ прихованість структури захищеної частини мережі для інших хостів;

+ надійна автентифікація й реєстрація минаючих повідомлень;

+ простіші правила фільтрації пакетів на мережному рівні, відповідно до яких маршрутизатор повинен пропускати тільки трафік, призначений для шлюзу прикладного рівня, і блокувати весь інший трафік;

+ можливість реалізації додаткових перевірок.

Недоліки шлюзів прикладного рівня:

- вища вартість, складність розробки, установки й налаштування;

- зниження продуктивності комп'ютерної мережі [2].

Аркуші доступу (access-lists)

Виконання функцій брандмауера також можна організувати за допомогою мережного фільтра на основі аркушів доступу. Вони визначають правила, за якими або дозволяється, або забороняється проходження трафіка з певними ознаками від одного мережного інтерфейсу маршрутизатора до іншого в середині самого маршрутизатора. Проте даний метод захисту має деякі недоліки, порівняно із міжмережевим екраном. Аркуші доступу дозволяють створити статичний однобічний фільтр, тоді як мережне з'єднання становить динамічний процес. Вони не дозволяють контролювати параметри IP-пакета, що залежать від попередніх пакетів. І найголовніше – це складність застосування аркушів доступу для тонкого налаштування фільтрації трафіка у відповідності із прийнятою політикою безпеки. Саме тому аркуші доступу не в змозі захистити систему від такого різновиду мережної атаки, як "викрадення з'єднання", або "хайджекінг" [1].

NAT. Network Address Translation

Ще одним методом захищеності мережі є "заміна мережної адреси" – Network Address Translation, або NAT. Вона полягає в заміні IP-пакету реальної адреси комп'ютера внутрішньої мережі на будь-яку іншу задану адресу при посиланні його в зовнішню мережу. Завдяки цьому внутрішня мережа отримує можливість використання діапазонів адрес, які не застосовуються в Інтернеті. Крім того, це дозволяє запобігти доступу інформації до внутрішніх комп'ютерів і приховує структуру мережі.

Різновидами (формами) NAT є:

- трансляція фіксованої внутрішньої адреси у фіксовану зовнішню.

Це найпростіший, але з погляду захисту найбільш марний метод, тому що зловмисник безперешкодно визначає такий комп'ютер у зовнішній мережі за певною зовнішньою адресою. Але вона необхідна при організації сервера, до якого потрібно забезпечити доступ ззовні.

- трансляція групи внутрішніх адрес в одну зовнішню.

Даний спосіб дозволяє всім внутрішнім комп'ютерам працювати з Інтернетом одночасно, а маршрутизатору розрізняти, кому яка відповідь транслюється за службовими даними TCP-з'єднання. У зовнішній мережі створюється враження, що до неї звертається тільки один комп'ютер. Таким чином, всі внутрішні комп'ютери приховані і зловмисник, навіть якщо бачить трафік, що виходить із внутрішньої мережі, не може визначити, від якого комп'ютера він виходить. Також за допомогою цього методу виключається можливість сканування ззовні внутрішньої мережі.

- використання для заміни внутрішніх адрес (не однієї адреси, а будь-якої з виділених).

Внутрішній комп'ютер, виходячи в Інтернет, одержує вільну у цей момент адресу з бази даних. При цьому адреси підмінюються динамічно, і кожне нове *TCP*-з'єднання може бути встановлене з іншою IP-адресою. Це також створює додаткові труднощі зловмиснику, тому що позбавляє його можливості атакувати будь-який внутрішній комп'ютер прицільно. Якщо запит приходить ззовні, то маршрутизатор не в змозі зв'язати адресу

бази даних з адресою мережі. Тому такий запит не досягне мети.

Proxy-сервер

Proxy-сервер («посередник») також підвищує рівень захищеності мережі, так як виключає необхідність прямого виходу в Інтернет комп'ютерів користувачів. З його допомогою стає можливим суворіший контроль за даними в IP-пакетах на рівні мережних додатків. Proxy-сервер працює як посередник між користувачем та мережним ресурсом в Інтернеті. Proxy-сервер складається із двох частин – клієнтської і серверної. Клієнтська частина слідкує за Інтернетом, серверна – за клієнтським комп'ютером. Коли клієнтський комп'ютер звертається до вилученого сайту через proxy-сервер, його клієнтський мережний додаток взаємодіє із серверною частиною proxy-сервера. При цьому proxy-сервер на рівні додатка передає клієнтський запит своєї клієнтської частини, і вона вже від імені proxy-сервера надсилає даний запит на вилучений сайт. Тобто відправлений IP-пакет має адресу proxy-сервера. Потім отримана відповідь передається у зворотну сторону від клієнтської частини proxy-сервера його серверної частини, з якою безпосередньо взаємодіє користувальницький комп'ютер. Таким чином, пряме з'єднання клієнтських комп'ютерів з вилученим сайтом виключається. Через те, що proxy-сервер працює тільки за декількома відомими протоколами (HTTP, FTP та інших) і не пропускає через себе інші пакети, він сильно обмежує можливості противника з використання мережних "троянських коней" для закріплення на будь-якому з користувальницьких комп'ютерів.

Антивірусний захист поштової системи

Однією з загроз інформації в комп'ютерній системі є загроза поштових вірусів. Іноді користувачу достатньо встановити покажчик на інфікований конверт, щоб вірус активізувався. Це дозволить зловмиснику таємно скачувати дані мережі та здобути всю інформацію, яка його цікавить. Запобігти цьому може антивірусний захист поштової системи [3;4]. Антивірусна система контролює повідомлення на поштових серверах на предмет наявності в них вірусів у процесі прийому та пересилання електронної пошти. Вся пошта, що проходить через сервер, спочатку перенаправляється спеціальному користувачу, у ролі якого виступає антивірусний процес. Він сканує зміст кожного аркуша на наявність у ньому фрагментів відомих вірусів. Якщо аркуш містить щось схоже на вірус, воно вилучається із процесу передачі й, залежно від налаштувань антивірусу, піддається заданій обробці. Повідомлення про виявлений вірус відсилаються відправнику й одержувачу інфікованого аркушу, а також на ім'я зазначених адміністраторів системи. Після перевірки аркуші, що не викликають підозри, відсилаються за призначенням.

Log-сервер

Log-сервер є загальновідомим механізмом протоколювання системних подій на серверах і клієнтських робочих станціях. Розробники програмного забезпечення включають у свої продукти фрагменти коду, які на ту чи іншу подію генерують відповідні текстові повідомлення, що посилаються операційній системі. Система збирає дані повідомлення в log-файлах, які потім можуть аналізуватися адміністратором або користувачем з метою з'ясування, які події відбувалися в системі деякий час потому [3].

Принцип роботи Log-серверу полягає в тому, що кожна операційна система може посилати повідомлення про системні події за UDP-протоколом на вилучений сервер. Це можуть робити також маршрутизатори та міжмережеві екрани. Збирання таких повідомлень на спеціально виділеному сервері забезпечує їх збереження від зловмисника. Тому для мінімізації ймовірності зламу log-сервер повинен бути призначений тільки для збору log-повідомлень і не повинен виконувати будь-які інші функції.

Висновки

Кожен з методів захисту інформації в комп'ютерних системах, підключених до мережі Інтернет, має свої переваги та недоліки, тому вибір певного методу залежить від напряму та специфіки роботи. Але попри все найбільш ефективнішим методом варто вважати міжмережевий екран (Firewall, брандмауер). Саме цей засіб захисту найкраще захистить комп'ютерну систему від несанкціонованого доступу та крадіжки інформації.

Література

1. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.

2. Милославская Н. Р. Интрасети: доступ в Интернет, защита / Н. Р. Милославская, А. И. Толстой. – М. : Юнити-Дана, 2000. – 527 с.

3. Столингс В. Криптография и защита сетей / В. Столингс. – М. : Вильямс, 2004. – 848 с.

4. Хорошко В. А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков. – К. : Юниор, 2003. – 504 с.

Literature

1. Kuznetsov O.O. Information protection in information systems / O.O. Kuznetsov, S.P. Yevseyev, O.G. King. – H. : Veed. KhNUE, 2011. - 512 p.

2. Myloslavskaya N.R. Yntrasety: access to the Internet, protection / N.R. Myloslavskaya, A.I. Tolstoy. – M. : Unity-Dana, 2000. - 527 p.

3. V. Stolynhs Cryptography and protection of networks / V. Stolynhs. – M. : Williams, 2004. - 848 p.

4. Khoroshko V.A. Methods and funds of the information protection / V.A. Khoroshko, A.A. Chekatkov. – K. : Yunyor, 2003. - 504 p.