УДК 006.9: 621.3

І.В. Рубан, Д.В. Сумцов, Д.В. Прибильнов, В.І. Новіков

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

АНАЛІЗ ІМОВІРНИХ ШЛЯХІВ ВИТОКУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ЗОВНІШНЬОГО НЕЗАХИЩЕНОГО СЕРЕДОВИЩА ПЕРЕДАЧІ ДАНИХ

У статті розглянуті шляхи та причини імовірного витоку конфіденційної інформації при використанні зовнішнього середовища для передачі даних. Приведений перелік імовірних загроз, які виникли у результаті перехоплення інформації. Наведені схеми передачі даних з використанням зовнішніх орендованих каналів, розглянуті шляхи протидії прослуховуванню мережевого трафіку.

Ключові слова: *інформаційна безпека, пасивна загроза інформації, шляхи витоку інформації, протидія пасивному прослуховуванню.*

Вступ

Сучасний розвиток інформаційних систем обумовлює необхідність захисту конфіденційної інформації, що передається між підмережами корпоративної мережі. Не існує абсолютно захищених систем. Саме це надає можливість пошуку та використання інформації у корисливих та неправомірних цілях.

Основний розділ

За даними сайту AV-test.org зростання кількості шкідливого програмного забезпечення відбувається у експоненційній залежності порівняно з попередніми роками (рис. 1).

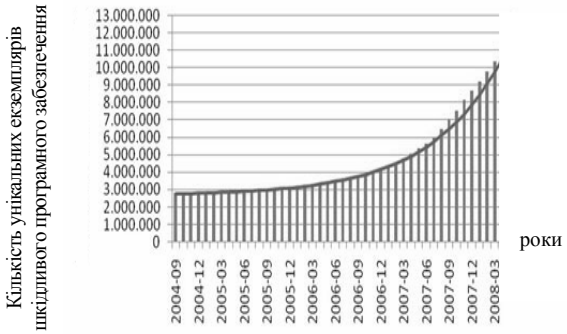

Рис. 1. Зростання кількості шкідливого програмного забезпечення

Проблема конфіденційності чітко стає перед жорстко визначеними та формалізованими інформаційними системами у зв'язку з різким зростанням потреб кінцевих користувачів у надходженні та обробці інформації у режимі реального часу. Побудова, налагодження та утримання власних систем передачі даних є дорогим та тривалим процесом, через це у якості середовища передачі даних використовуються зовнішні виділені канали, що орендуються у телекомунікаційних компаній, або, як варіант, використовується Інтернет. Схема передачі даних через зовнішнє середовище зображена на рис. 2.

Захист інформації в процесі її передачі по відкритих каналах ґрунтується на використанні віртуальних захищених мереж VPN. Віртуальною захищеною мережею VPN (Virtual Private Network) називають об'єднання локальних мереж і окремих комп'ютерів через відкрите зовнішнє середовище передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних.

Віртуальна захищена мережа VPN формується шляхом побудови віртуальних захищених каналів зв'язку, що створюються на базі відкритих каналів зв'язку загальнодоступної мережі.

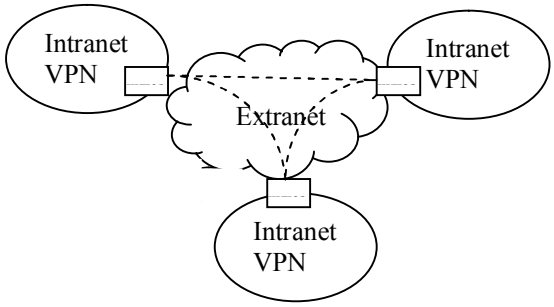

Рис. 2. Схема передачі даних через зовнішнє середовище

У основі концепції побудови віртуальних захищених мереж VPN лежить досить проста ідея: якщо в глобальній мережі є два вузли, яким потрібен обмін інформацією, то між цими двома вузлами необхідно побудувати віртуальний захищений тунель для забезпечення конфіденційності і цілісності інформації, яка передається через відкриту мережу. Доступ до цього віртуального тунелю має бути неможливий або надзвичайно ускладнений можливим активним і пасивним зовнішнім спостерігачам. Основний принцип захисту від зовнішньої небезпеки полягає у створенні умов за яких інформація буде доступна визначеним користувачам та максимально недоступна всім іншим.

За умови необхідності сильного захисту інформації використовується поєднання орендованих виділених каналів зв'язку та віртуальних приватних мереж VPN із використанням шифрування.

У результаті аналізу було виявлено, що ділянкою, яка становить найбільшу загрозу у запропонованій схемі на рис. 2, є Extranet, тобто зовнішнє середовище, яке використовується для передачі даних між під мережами.

Під загрозою безпеці інформації зазвичай розуміють потенційно можливу подію (дію, процес або явище), яка може привести до нанесення шкоди безпеці інформації.

При передачі даних через зовнішнє середовище з використанням шифрування, мереж VPN або прямого виділеного підключення, дані вже піддаються загрозі через те, що зовнішнє середовище неможливо контролювати. Єдине, що можливо – відстежувати стан інформації, що передається, на кінцевих пристроях. Деталізована схема передачі даних із використанням зовнішніх орендованих каналів наведена на рис. 3.

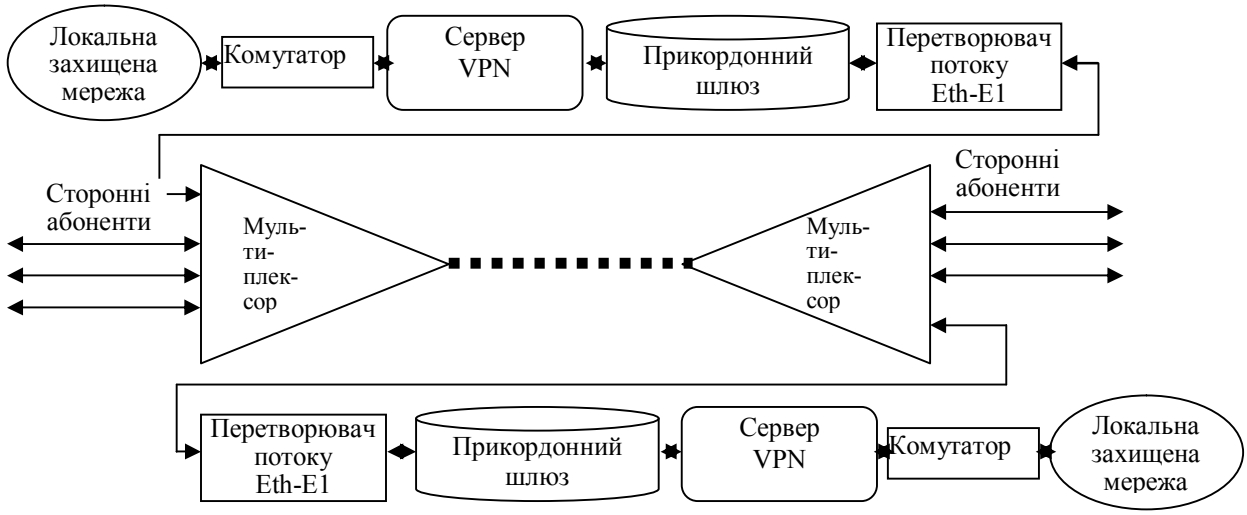

Рис. 3. Схема передачі даних з використанням зовнішніх орендованих каналів

Наведена схема є найбільш захищеною, але навіть за таких обставин присутність сторонньої інформації від зовнішніх абонентів робить задачу забезпечення інформаційної безпеки актуальною. Особливу загрозу представляє шлях між мультиплексорами (рис. 3) через невизначеність шляхів передачі даних від вихідного пристрою передачі даних до вхідного. Відсутність можливості контролю за фізичними пристроями породжує першу і основну інформаційну загрозу: «сніфінг» – прослуховування мережевого трафіку.

Прослуховування мережевого трафіку є пасивною мережевою загрозою і використовується для отримання мережевого пакетного трафіку та подальшого аналізу отриманих пакетів даних.

Після того, як зловмисником була отримана вихідна інформація, у результаті її аналізу можуть бути виявлені наступні характеристики інформаційної системи:

1. Кількість вузлів, що обмінюються повідомленнями.
2. Внутрішній діапазон мережевих адрес.
3. Наявність серверів.
4. Найменування використаного програмного забезпечення та його версію.
5. Характер інформації, що передається.
6. Можливість перехоплення та декодування паролів.

При отриманні даного роду відомостей виникає можливість отримання прав та привілеїв адміністратора мережі, що, у свою чергу, робить можливим наступні дії:

1. Виток інформації.
2. Зміна (модифікація) інформації.
3. Втрата інформації (не надходження інформації до отримувача).

Крім цього, зловмисник має можливість встановлення альтернативних способів входження та авторизації у системі, тобто встановлення шкідливого програмного забезпечення типу backdoor або програм «демонів», які в автоматичному режимі будуть відслідковувати операції всередині системи та за необхідності відправляти інформацію за потрібними зловмиснику адресами.

Знизити загрозу використання даних мережевого трафіку можна за допомогою наступних заходів:

1. Аутентифікація. Сильні засоби аутентифікації є найважливішим способом захисту від використання інформації, яка була здобута шляхом перехоплення пакетів. Під "сильними" розуміються такі методи аутентифікації, які важко обійти. Прикладом такої аутентифікації є одноразові паролі (One-Time Passwords, OTP). OTP – це технологія двохфакторної автентифікації, при якій відбувається поєднання матеріального ключа з відомим користувачу паролем. Типовим прикладом двохфакторної аутентифікації є робота банкомату, який ідентифікує користувача, по-перше, за його пластиковою карткою, а по-

друге, за PIN-кодом, який вводився. Для автентифікації у системі OTP також потрібний PIN-код і особиста картка. Під "карткою" (token) розуміється апаратний або програмний засіб, що генерує за випадковим принципом унікальний одномоментний одноразовий пароль. Якщо шляхом прослуховування пароль буде викрадений, інформація вже буде непотрібною, оскільки на даний момент викрадений пароль використаний та виведений із вжитку. Цей спосіб боротьби із використанням мережевого трафіку ефективний лише у випадку перехоплення паролів. При перехопленні іншої інформації (наприклад, повідомлень електронної пошти), засоби перехоплення трафіку не втрачають своєї ефективності.

2. Комутована інфраструктура. Ще одним способом боротьби з прослуховуванням пакетів у мережевому середовищі є створення комутованої інфраструктури. Якщо в усій організації використовується комутований Ethernet, то може бути отриманий доступ лише до трафіку, що надходить на той порт, до якого підключений зловмисник. Комутована інфраструктура не усуває загрози прослуховування мережевого трафіку, але помітно знижує її імовірність.

3. Криптографія. Найефективніший спосіб боротьби з прослуховуванням трафіку, який хоч і не запобігає перехопленню та не розпізнає роботу мережевого аналізатора, але робить цю роботу даремною. Якщо канал передачі даних є криптографічно захищеним, то зловмисник перехоплює не повідомлення, а зашифрований текст. Наприклад, криптографія Cisco на мережевому рівні базується на протоколі IPSec, який є стандартним методом захищеного зв'язку між пристроями засобами стеку протоколів TCP/IP.

4. Четвертий спосіб боротьби із мережевим прослуховуванням трафіку полягає в установці апаратних або програмних засобів, що розпізнають працюючі у мережі засоби прослуховування. Дані засоби не можуть повністю ліквідовувати загрозу, але, як і багато інших засобів мережевої безпеки, включаються у загальну систему захисту. Засоби розпізнавання прослуховування вимірюють час реагування хостів і визначають, чи не доводиться хостам обробляти зайвий трафік. Один з таких засобів, розроблений компанією LOpht Heavy Industries, має назву AntiSniff.

Висновки

З проведеного аналізу можна зробити висновок, що за умові використання будь-якого зовнішнього середовища, інформація, що передається піддається ризику перехоплення, що у свою чергу робить можливими впливи на вихідну систему. Найбільш імовірною ознакою комп'ютерної розвідки у зовнішньому середовищі є проведення прослуховування мережевого трафіку. Основною причиною для цього є відсутність контролю зовнішнього середовища. Для подолання пов'язаних із перехопленням мережевих пакетів загрозою актуальним представляється задача розробки методів виявлення факту прослуховування мережевого трафіку.

Список літератури

1. Защита информации в компьютерных сетях. Практический курс: уч. пособ. / А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский и др.; под ред. Н.И. Синадского. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.

2. Эриксон Д. Хакинг: искусство эксплойта / Д. Эриксон: пер. с англ. – СПб: Символ-Плюс, 2005. – 240 с.

3. Шаньгин В.Ф. Информационная безопасность компьютерных сетей и систем: уч. пособ. / В.Ф. Шаньгин. – М.: ИД «Форум»: Инфра М, 2008. – 416 с.

4. Проблемы безопасности вертуальных частных сетей [Электрон. ресурс]. – Режим доступа: http://www.internet-technologies.ru.

5. Вертуальные частные сети [Электрон. ресурс]. – Режим доступа: http://vpn.ru/.

Надійшла до редколегії 11.10.2011

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

АНАЛИЗ ВЕРОЯТНЫХ ПУТЕЙ УТЕЧКИ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ВНЕШНЕЙ НЕЗАЩИЩЁННОЙ СРЕДЫ ПЕРЕДАЧИ ДАННЫХ

И.В. Рубан, Д.В. Сумцов, Д.В. Прибыльнов, В.І. Новиков

В статье рассмотренные пути и причины вероятной утечки конфиденциальной информации при использовании внешней среды для передачи данных. Приведен перечень вероятных угроз, которые возникли в результате перехвата информации. Приведены схемы передачи данных с использованием внешних арендованных каналов, рассмотрены пути противодействия прослушиванию сетевого трафика.

Ключевые слова: *информационная безопасность, пассивная угроза информации, пути утечки информации, противодействие пассивному прослушиванию.*

ANALYSIS OF WAYS OF INFORMATION LOSS AT THE USE OF UNPROTECTED ENVIRONMENT OF DATA COMMUNICATION

I.V. Ruban, D.V. Sumtsov, D.V. Pribylnov, V.I. Novikov

In the article the considered ways and reasons of credible loss of confidential information at the use of environment for communication of data. A list over of credible threats that arose up as a result of intercept of information is brought. Charts over of communication of data are brought with the use of the external leased circuits, the ways of counteraction to listening of network traffic are considered.

Keywords: *informative safety, passive threat of information, way of loss of information, counteraction to the passive listening.*