ВИБІР ПОЛІТИКИ БЕЗПЕКИ В КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ МЕРЕЖАХ. ВИКОРИСТАННЯ VPN-ТУНЕЛІВ ТА МЕРЖЕВОГО ЕКРАНУ

Трапезон К. О., к.т.н.; Панічева Н. О.;Гумен Т. Ф.
Національний технічний університет України
«Київський політехнічний інститут», м. Київ, Україна

Пропорційно до збільшення частки населення, що використовує світову мережу Інтернет як джерело доступу до інформації в повсякденному житті та в комерційних цілях, кожен день зростає кількість атак, що ставить під сумнів існуючі базові принципи мережної безпеки [1].

Основна задача, з якою стикаються всі кваліфіковані спеціалісти — первинне визначення типу можливих порушень мережевої безпеки [2–4]. Метою статті є формулювання принципів та кроків, які дозволяють розв'язати проблему захисту інформації в телекомунікаційних мережах загального та індивідуального доступу, а також демонстрація одного з можливих варіантів.

Для успішного вибору політики захисту необхідне виконання наступних кроків: визначення необхідного рівня захисту мережі, виявлення головних причин проблем, що виникають при захисті мережі, надання характеристики порушників захисту та виявлення мотиви їх дій, ідентифікація типових загроз безпеки мережі,вибір контрмір, за допомогою яких вирішуються задачі.

Серед головних причин проблем захисту мережі можна виділити:

1) технологічні недоліки мережі: вразливі місця та недоліки операційних систем, мережевого обладнання, протоколів передачі даних;

2) недоліки конфігурації: недостатній захист, що забезпечується налаштуваннями за замовчуванням; неправильна конфігурація мережевого обладнання; незахищені облікові записи користувачів; або використання ними занадто простих паролів; неправильні налаштування служб Internet;

3) недоліки політики безпеки: відсутність документованої політики захисту; внутрішні протиріччя; відсутність спадковості; відсутність логічного контролю доступу до мережевого обладнання; необережне адміністрування; моніторинг та контроль; необізнаність про можливість атак, невідповідність програмного забезпечення та апаратних коштів прийнятої політики захисту мережі; відсутність процедур проведення обробки інцидентів захисту та плану відновлення системи.

З-поміж величезної кількості існуючих рішень із захисту комп'ютерних мереж, слід зазначити найбільш «універсальні»: патчі та оновлення програмного забезпечення (ПЗ), засоби блокування спливаючих вікон, захист від шпіонського ПЗ, антивірусні програми, мережевий

фільтр, спам-фільтр, шифрування паролів, використання *VPN*-тунелів, відключення потенційно небезпечних служб маршрутизаторів і т. д.

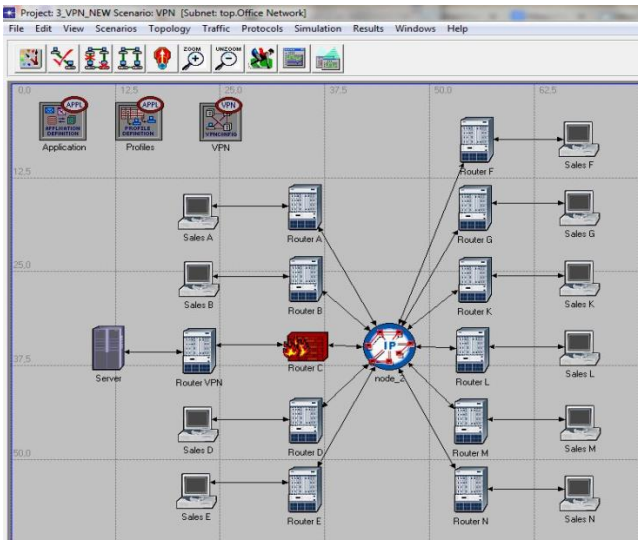

Рисунок 1. Робоче вікно програми Modeler і змоделлю комп'ютерної мережі з мережевим екраном і налаштованими *VPN*-тунелями

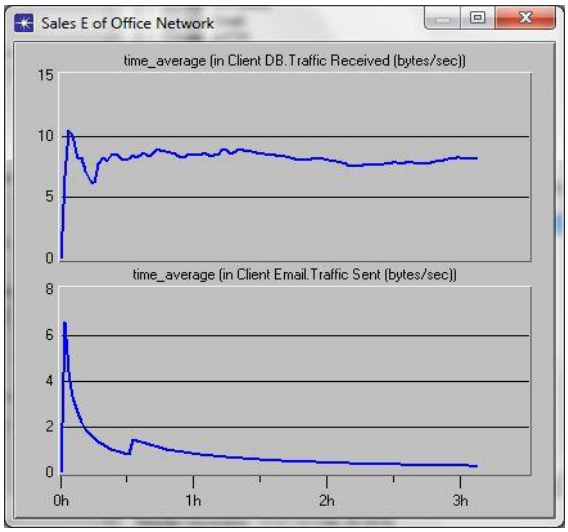

Рисунок 2. Результат роботи робочої станції *Sales E* з настроєним *VPN*-тунелем

Проілюструємо запровадження окремих заходів політики безпеки на апаратному та програмному рівнях в програмі Modeler. На рисунку 1 показано варіант моделі комп'ютерної мережі з політикою безпеки, основаною на включенні мережного екрану та налаштуванні VPN-підключень. За умови збільшення рівнів вхідного та вихідного трафіку є можливість унеможливити передачу даних до окремих вузлів моделі.

За результатами відпрацювання моделі можна порівняти дані для підключення робочої станції *Sales F* без *VPN* тунелю та робочої станції *Sales E* з налаштованим *VPN*-тунелем. Як бачимо, *Sales F* не пропускає трафік на додаток *Database* та не отримує трафік з додатку *E-mail*, в той час, як додатки на *Sales E* працюють у звичайному режимі (рис. 2).

Таким чином, згідно описаної вище політики безпеки, можна встановити обмеження доступу до серверів та ресурсів мережі для окремих вузлів і навіть за окремими видами даних, що передаються в мережі офісного масштабу.

Окремо до політики безпеки на апаратному рівні можна встановити мережевий екран (фаєрвол) (рис. 1), який дозволяє на основі описаного профілю користувачів закрити доступ до ресурсів мережі. Слід відмітити, що за налаштуваннями моделі в програмному середовищі *Modeler* не використовується доступ на основі персоналізованих даних користувачів, а це значно спрощує архітектуру мережі, адже при цьому зникає необхідність встановлювати на рівні управління персоналізованих баз даних користувачів мережі.

Перелік посилань

1. Девянин П. М. Модели безопасности компьютерных систем / П. М. Девянин. — М.: Академия, 2005. — 144 с.–ISBN 5-7695-2053.

2. Андрончик А. Н. Защита информации в компьютерных сетях. Практический курс / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский и др.; под ред. Н. И. Синадского. — Екатеринбург: УГТУ-УПИ, 2008. — 248 с.: 153 ил., 14 табл. – Библиогр.: с. 239-240. –ISBN978-5-321-01219-2.

3. Каторин Ю. Ф.Защита информации техническими средствами. Учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак. — Санкт-Петербург: НИУ ИТМО, 2012. — 416 с.−ISBN978-5-321-01219-2.

4. Биячуев Т. А. Безопасность корпоративных сетей. Учебное пособие / Т. А. Биячуев. — Санкт-Петербург. ГУ-ИТМО, 2004. — 161 с.

Анотація

Визначено основні кроки, які дозволяють при проектуванні телекомунікаційних мереж забезпечити захист даних через формулювання та дотримання правил політики безпеки. Сформульовано основні фактори, які можуть призвести до зменшення рівня захисту комп'ютерних інформаційних мереж. Перераховані загальні заходи безпеки та проілюстровано один із методів.

Ключові слова: інформація, політика безпеки, захист мережі, типи загроз.

Аннотация

Определены основные шаги, которые позволяют на этапе проектирования телекоммуникационных сетей обеспечить защиту данных путем формулирования и выполнения правил политики безопасности. Сформулированы основные факторы, которые могут привести к снижению уровня защиты компьютерных информационных сетей. Перечислены общие меры безопасности и проиллюстрировано один из методов.

Ключевые слова: информация, политика безопасности, защита сети, типы угроз.

Abstract

Basic steps that allow on the stage of planning of telecommunications network to provide the protection of data by formulation and implementation of rules of policy of safety are certain. Basic factors that can result in the decline of level of defense of computer informative networks are set forth. Common security solutions were listedand one of the methods was illustrated.

Keywords: information, security policy, protection of the network, types of threats.