захисту локального мережевого сховища потрібно використовувати комплексні методи захисту.

Мисливець Д. О.,
Криворізький національний університет
Кумченко Ю. О.
к.т.н., доцент, Криворізький національний університет

СИСТЕМА ЗАХИСТУ КОМП'ЮТЕРІВ МЕТОДОМ ФІЛЬТРАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

Розглянуто актуальність використання брандмауеру для користувачів комп'ютерів. Представлено розмежування контент-фільтрів та класифікацію фільтрації.

У зв'язку з розвитком різносторонніх оновлених мережевих технологій збільшується обсяг інформації, яка передається мережею, а також появою нових протоколів передачі даних прикладного рівня, тому все більшої актуальності в наш час набуває метод фільтрації цього трафіку.

Файєрвол, брандмауер чи мережевий екран – це пристрій забезпечення мережевої безпеки, що здійснює моніторинг вхідного та вихідного трафіку, на базі певних, встановлених правил безпеки, приймаючи рішення про дозвіл чи заборону трафіку в мережі [1]. Реалізація відбувається шляхом використання певного програмного, апаратного, або програмно-апаратного забезпечення. Застосовується як спосіб, щоб забезпечити захист комп'ютера від різноманітних мережевих атак, таких як: шпигунські програми, DDoS-атаки тощо; блокування відвідування заражених вірусами або небажаних інтернет-сайтів; виявлення різноманітних шпигунських засобів стеження за активністю користувача.

ПАРАМЕТРИ КОНТЕНТ-ФІЛЬТРІВ

Системи фільтрації мережевого трафіку можна розділити на такі показники:

1. Підзвітність. Оцінює кількість участі населення в політиці фільтрації контенту.

2. Відкритість. Дає можливість користувачу отримати перевірену інформацію про відвідування ресурсу, який віднесений до заборонених.
3. Точність. Відповідає за успішність цензури (тобто надмірне або ж недостатнє блокування)
4. Прозорість. Надання параметрів, котрі дозволяють віднести трафік до забороненого.

КЛАСИФІКАЦІЯ ФІЛЬТРАЦІЇ ТРАФІКУ

1. Міжнародний рівень. Фільтрація DNS-запитів на державному рівні.
2. Рівень інтернет-шлюзу. Потребує інсталяції програмного забезпечення (ПЗ), що забезпечить фільтрацію. Метод зберігає швидкість інтернет-доступу. Використовується приватними підприємствами та державними організаціями.
3. Рівень інтернет-провайдерів. Для даної фільтрації використовуються переліки заборонених сайтів, які сформувались судами та державними службами. Метод визнаний надійним.
4. Рівень комп'ютера користувача. ПЗ інсталюється на комп’ютер. Метод вважається ефективним для домашнього використання, а також для застосування на невеликих підприємствах. Є доступним рішення.

ВИСНОВКИ

Таким чином, фільтрація мережевого трафіку є необхідною для кожного користувача комп’ютера. На сьогодні один із методів захисту від комп'ютерних зловмисників є саме міжмережевий екран. І хоча він не гарантує повноцінний захист від професійних хакерів, але все ж таки ускладнює їм отримати доступ до конфіденційної інформації.

ЛІТЕРАТУРА

1. Что такое межсетевой экран? – URL: https://www.cisco.com/c/ru_ru/products/security/firewalls/what-is-a-firewall.html (дата звернення: 20.02.2019).