УДК 004.77

ПРОБЛЕМИ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

Воргуль О., Білоцерківець О. Г., Сєріков А. О.
Харківський національний університет радіоелектроніки, м. Харків

Віддалений доступ є однією з найпоширеніших тенденцій у сучасних комп'ютерних середовищах. Простота доступу до внутрішніх приватних мереж через Інтернет за допомогою телекомунікаційних пристроїв породила занадто багато загроз безпеці для кінцевих пристроїв. Дані, що перебувають на кінцевій точці віддаленого доступу не мають повного захисту між шлюзом VPN та внутрішніми ресурсами.

Remote access is one of the most common trends in today's computer environment. The ease of access to internal private networks over the Internet through telecommunications devices has posed too many security threats to end devices. Data at the remote access endpoint does not have full protection between the VPN and internal resources.

Методи віддаленого доступу мають ряд проблем з безпекою, які роблять їх неефективними при розгортанні VPN. Почнемо з того, що тунельований IP-трафік може не отримати намічений рівень перевірки або застосування політики мережевими пристроями безпеки, якщо такі пристрої не підтримують тунелювання. Це знижує глибоку захист і може викликати проломи в безпеці.

Цей недолік безпеки відноситься до всіх пристроїв, розташованим в мережі, і до будь-яких міжмережевих екранів на основі кінцевих хостів, існуючі механізми перехоплення не показують їм потік IP-пакетів після того, як тунельний клієнт виконує декапсуляцію або до того, як він виконає інкапсуляцію. Крім того, IP-адреси всередині тунелів не підлягають вхідної та вихідної фільтрації в мережі, через яку вони тунелюються, і, отже, можуть пропускати шкідливий контент у внутрішні мережі.

Більш того, якщо інкапсульований IP-пакет вказує вихідну маршрутизацію за межами одержувача тунельного клієнта, хост може переслати IP-пакет на вказаний наступний перехід. Це може бути несподіваним і таким, що суперечить побажанням адміністратора, а також може обійти елементи управління маршрутизацією від джерела в мережі.

Крім того, багато підприємств дозволяють, або не регулюють використання сторонніх сервісів зберігання файлів для полегшення віддаленого доступу до даних, а коли файли потрапляють в хмарні репозиторії, підприємства втрачають контроль. Зі свого боку, прямий доступ до додатків вимагає використання IPv6 виключно для розподілу адресації між підключе-

ними кінцевими точками. Коли справа доходить до адресації і ідентифікації клієнтів, це являє собою більш серйозну проблему управління.

Для вирішення деяких з цих проблем був розроблений ряд протоколів. На жаль, ці протоколи також містять уразливості, які роблять їх небезпечними. Наприклад, протокол RFB, протокол відображення, має деякі недоліки безпеки, включаючи вразливість для атаки Man-In-The-Middle.

Незважаючи на те, що протокол RFB використовує зашифровані паролі і мережу, будь-який обмін даними по мережі вразливий і може бути атакований MITM з використанням спец. інструментів і методів. Крім того, додатки VNC, розроблені на основі протоколу RFB, зазвичай повільніші, пропонують менше функцій і варіантів безпеки, ніж віддалений робочий стіл (RD), який заснований на протоколі .

Хоча дані, що відправляються між сервером і клієнтом, зашифровані, протокол RDP може бути підданий атаці Man-In-The-Middle, оскільки під час налаштування ключів шифрування для сеансу не виконується перевірка сервера.

Інформаційні джерела

1. Шальгин В.О., Комплексний захист корпоративної інформації. Навч.пос. 2009. 404 с.

2. Биячуев Т.А. / під ред. Л.Г.Осовецкого, Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004. - 161 с.

АНАЛІЗ АТАК НА БАЗИ ДАНИХ ТА МЕТОДИКА ЗАХИСТУ

Масник С. Т., Шабатура М.М.
Національний університет «Львівська політехніка», м. Львів

У роботі розглянуто актуальну проблему на сьогоднішній день, це атаки на бази даних. Проаналізовано три найпоширеніших атаки: SQL-ін'єкції, «Meow» та атаку методом грубої сили. Запропоновано рекомендації щодо зниження шансів реалізації атак.

Ключові слова: *бази даних, атаки, захист баз даних*

In the paper was considered a major problem of our time, it is database attacks. There are three most common attacks: SQL injection, "Meow" attack and the brute force. Recommendations for reducing the chances of attack implementation are offered.

Keywords: *databases, attacks, database protection*

Цифрова трансформація суспільства спричинила неабиякий технічний прогрес у всіх сферах людського життя. Проте, окрім безумовного спрощення буденних справ та багатократного зменшення паперової тяганини, це стало каталізатором розвитку здібностей кіберзлочинців, оскільки зараз впливовість вимірюється терабайтами конфіденційної інформації.