Кльоц Ю.П., , к.т.н., доцент
Кукурудза Д.М., здобувач
Хмельницький національний університет

МЕТОДИ ВИЯВЛЕННЯ АТАК В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Комп'ютерні мережі набули широкого розвитку паралельно з їх розвитком активно розвивається шкідливе програмне забезпечення та методи і засоби реалізації атак на та в комп'ютерних мережах. За методами атак також розвиваються і методи їх виявлення або недопущення.

Розвиток мереж та специфіка їх використання впливає і на особливості мережі. Серед відомих мереж можна виділити такі: корпоративні мережі, корпоративні мережі з BYOD, локальні мережі, публічні мережі з відкритим доступом.

Корпоративні мережі характеризуються високим рівнем контролю та управління, обмеженим доступом шляхом автентифікації та авторизації, використанням захищених сегментів VLAN, наявними засобами моніторингу та аналізу трафіку, політиками безпеки для користувачів та пристроїв, захистом від зовнішніх загроз (брандмауери, IDS/IPS), використанням централізованого управління (AD, SIEM, NAC).

Корпоративні мережі з BYOD характеризуються змішаним використання корпоративних та особистих пристроїв, динамічною IP-адресацією та ізоляцією пристроїв, використанням NAC для контролю доступу, високим ризиком зараження мережі через особисті пристрої, необхідністю обов'язкової сегментації та моніторингу трафіку, політиками безпеки на основі MDM, Zero Trust, контроль доступу, використанням VPN або контейнеризації даних.

Локальні мережі характеризуються висока швидкість передачі даних, відносно низьким рівнем безпеки, обмеженим будівлею або кампусом радіусом дії, центральним або децентралізованим контролем трафіку, використанням VLAN для поділу сегментів, основний фокус – продуктивність і стабільність.

Публічні мережі з відкритим доступом характеризуються відсутністю або мінімальним контролем доступу, високим ризиком атак (MITM, фішинг, підміна DNS), використанням загальних IP-адрес, відсутністю або слабким шифруванням трафіку, відкритим підключенням через Wi-Fi або Ethernet, високим рівнем анонімності користувачів, обмеженою пропускною здатність через велике навантаження.

Проведемо аналіз відомих методів та підходів до виявлення атак в комп'ютерних мережах.

Таблиця 1 Методи та підходи до виявлення атак в мережах.

Метод виявлення атак	Корпоративні мережі	Корпоративні з BYOD	Локальні мережі	Публічні мережі
Сигнатурний аналіз (IDS/IPS)	Добре	Середньо	Добре	Погано
Аналіз поведінки (UEBA)	Добре	Добре	Середньо	Погано
Моніторинг NetFlow/DPI	Добре	Добре	Добре	Погано
Моніторинг кінцевих пристроїв (EDR)	Добре	Добре	Середньо	Погано
Контроль доступу NAC	Добре	Добре	Середньо	Погано
Фільтрація DNS/блокування загроз	Добре	Добре	Добре	Добре
Аналіз логів (Syslog, SIEM)	Добре	Добре	Середньо	Погано
Виявлення DDoS-атак	Добре	Добре	Добре	Добре
Моніторинг Wi-Fi (WIPS/WIDS)	Середньо	Добре	Погано	Добре
Виявлення MITM-атак	Добре	Добре	Середньо	Добре

В комірках таблиці вказано наскільки ефективно використовувати розглянуті методи в різних типах мереж. Окрім цього при виборі методів виявлення атак необхідно враховувати вартість апаратного та програмного забезпечення, вимоги до мережевого обладнання, ресурсоємкість, скляність розгортання та підтримки системи.

Представлений в таблиці 1 аналіз методів вказує, що більшість з них орієнтовані на використання в корпоративних мережах. Сегменту локальних мереж приділена менша увага, оскільки здебільшого такі мережі є ізольованими від інтернету.

Методи виявлення атак зазвичай не орієнтовані на публічні мережі, оскільки вони будучи достатньо чисельним зазвичай не можуть використовувати дорогі програмно-апаратні комплекси та не мають можливості постійної підтримки та реакції на нові загрози.

Тому доцільним є розробка нових методів виявлення атак в публічних комп'ютерних мережах.

Список використаних джерел:

1. Scarfone, K., & Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST, 2007.
2. Chandola, V., Banerjee, A., & Kumar, V. Anomaly Detection: A Survey. ACM Computing Surveys, 2009.