УДК 004.7
А.М. Ребуха
(Тернопільський національний технічний університет імені Івана Пулюя)

ПОРІВНЯЛЬНЕ ДОСЛІДЖЕННЯ РОБОТИ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ У РОБОТУ ІНФОРМАЦІЙНИХ СИСТЕМ

UDC 004.7
A.M. Rebukha

COMPARATIVE RESEARCH OF INTRUSION DETECTION SYSTEMS AND INTRUSION PREVENTION SYSTEMS OPERATION IN INFORMATION SYSTEMS

На сьогодні системи виявлення (Intrusion Detection Systems – IDS) та запобігання вторгнень (Intrusion Prevention Systems – IPS) є невід'ємними складовими для впровадження засобів та заходів безпеки у будь-яку інформаційну систему [1,2]. Використання цих систем ґрунтується на способі реакції на атаку [3]. Не завжди потрібно мати докладні відомості про вторгнення, іноді досить отримати сповіщення про нього.

IDS моніторить мережу на предмет можливих небезпек. При виявленні проблеми IDS сповіщає адміністратора про це. Існує декілька типів IDS та декілька методів виявлення вторгнень. Типи IDS:

1. Мережева система виявлення вторгнень (Network IDS – NIDS) відслідковує вхідні та вихідні пакети даних по всій мережі чи в частині її вузлів.
2. Система виявлення вторгнень на хості (HostIDS – HIDS) відслідковує лише один з вузлів інформаційної системи (комп'ютер чи пристрій).

Методи виявлення вторгнень:

1. На основі сигнатур. Робота таких IDS базується на наперед складеному спискові відомих програмних загроз та властивих їм поведінкових проявів.
2. На основі аномалій. Робота цієї системи базується на моделі нормальної поведінки інформаційної системи та сповіщенні адміністратора про відхилення від моделі нормальної поведінки.

Системи запобігання вторгнень (IPS) використовуються для автоматизації реакції системи на загрози інформаційної безпеки. Тому розглядають такі типи IPS:

1. Мережеві (Network) IPS (NIPS) на основі сигнатур небезпек.
2. Аналізатори поведінки мережі (NBA) виявляють аномалії в роботі мережі. Тому вони вимагають початкової фази навчання.

Література.

1. Olexander Shmatko, Svitlana Balakireva, Andrii Vlasov, Nataliya Zagorodna, Olha Korol // Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 2020. Vol. 3. Issue 9 (105), pp. 6–19.
2. А. М. Стефанів, Н. В. Загородна, Р.О. Козак // Класифікація методів виявлення фішингу в інтерактивних мультимедійних виданнях. VIII Міжнародна науково-технічна конференція молодих учених та студентів "АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ" (27–28 листопада 2019 року). p. 69.
3. Serhii Yevseiev, Volodymyr Aleksiyev, Svitlana Balakireva, Yevhen Peleshok, Oleksandr Milov, Oleksii Petrov, Olena Rayevnyeva, Bogdan Tomashevsky, Ivan Tyshyk, Olexander Shmatko // Development of a Methodology for Building an Information Security System in the Corporate Research and Education System in the Context of University Autonomy. Eastern-European Journal of Enterprise Technologies, 2020. Vol. 3. Issue 9 (105), pp. 49–63.