Секція 2

АНАЛІЗ ВРАЗЛИВОСТЕЙ SCADA-СИСТЕМ

Єлюхін Р. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»,
Харків, Україна
Науковий керівник Землянко Г. А.

Актуальність. Об'єм ринку SCADA-систем у 2019 році привісив 30 мільярдів доларів та, по оцінкам, буде зростати у період до 2026 року по 7.5% на рік. Такий стрімкий ріст обумовлюється широким впровадженням SCADA-систем у інфраструктуру промислового, міського та транспортного IoT. Основний попит на SCADA-системи, все також, йде від критично-важливих інфраструктур, таких як: енергетика, нафтова та газова промисловість, телекомунікації, хімічна та фармацевтична промисловості [1]. Однак з розвитком ринку розвивається і загальна кількість вразливостей, виявлених у компонентах АСУ ТП, так у 2017 році ця кількість досягала 197, а вже у 2018 році зросла до 257 виявлених вразливостей, серед яких найбільшу частку у 23% займають вразливості SCADA-систем [2]. З сучасних загроз можна відмітити атаку на українське обленерго у 2016 році, водоочисну станцію у Флориді та енергопостачання Мумбаю у 2021 році [3].

Також на даний момент не існує єдиного методу визначення рівня захищеності SCADA-систем, який би дозволяв визначати проблеми з різних сторін [4].

Метою даної роботи є виявлення слабких місць SCADA-системи та оцінки рівня її захищеності.

Основні положення. Огляд стану безпеки АСУ ТП, проведений компанією Positive Technologies показує, що кожна п'ята вразливість усувається довше за місяць. 50% вразливостей дозволяють хакеру запустити виконання коду. Для 35% вразливостей є експлойти. Серед усіх вразливостей АСУ ТП SCADA-вразливості займають найвищу долю [5].

Аналізуючи типи вразливостей SCADA-систем серед найбільш застосовуваних можна відмітити:

− Вразливості автентифікації, які зв'язані з "слабким" парольним захистом. До таких вразливостей відносять - використання стандартних інженерних паролів, встановлених виробниками на приладах промислової автоматики, використання простих паролей, зберігання паролей у відкритих джерелах.

– Вразливості програмно-апаратних компонентів, зв’язані з використанням відкритих портів системи та проведенням DoS-атаки для переповнення розміру буферів.

Висновки. Основною ціллю атаки на АСУ ТП стають SCADA-системи, тому забезпечення безпеки SCADA-систем одне із головних завдань, яке стоїть перед підприємством, в якому функціонує така система. Серед проблем захищеності SCADA-систем можна відмітити те, що для атаки зловмиснику часто не потрібно володіти складними навичками, бо серед найпоширеніших SCADA-вразливостей найбільші частки займають вразливості поганого захисту паролей. Також слід відмітити, що у більшості випадків актуального захисту від проникнення в програмне забезпечення АСУ ТП не дозволяє побудувати не відсутність інформації про вразливості ПЗ, а відсутність регламентуючої законодавчої бази, єдиних міжнародних стандартів, щоб несли обов'язковий, а не рекомендаційний характер.

Список літератури

1. A. Bhutani, P. Wadhwani. SCADA Market Size By Component, By Applicatio n, Industry Analysis Report, Regional Outlook, Growth Potential, Competitive Mar ket Share & Forecast, 2020 – 2026, 2020. – 160 с. *Global Market Insights.* URL – https://www.gminsights.com/industry-analysis/scada-supervisory-control-and-data-acquisition-market (дата звернення: 17.11.2021);
2. Вразливості в АСУ ТП, за 2018 рік. *Positive technologies.* URL – https://www.ptsecurity.com/ru-ru/research/analytics/ics-vulnerabilities-2019 (дата звернення: 18.11.2021);
3. Атаки за участю SCADA-систем. *SecurityLab.ru.* URL – https://www.securitylab.ru/news/tags/SCADA (дата звернення: 18.11.2021);
4. O. Syrotkina, M. Alekseyev, O. Aleksieiev. Evaluation to Determine the Efficiency for the Diagnosis Search Formation Method of Failures in Automated Systems. Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 4, Issue 9 (88). – P. 59-68. *PDF*. URL – https:// pdfs.semanticscholar.org/bde9/dab572e7cf8e57d17ee3fee344e0d51ad35c.pdf (дата звернення: 19.11.2021);
5. Сироткіна Є.І. Структурно-логічна модель діагностики відмов SCADA системи. Науковий вісник НГУ. – 2014. – № 4. – С. 52-57.

Відомості про авторів

Єлюхін Роман Валерійович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 068-756-69-94, r.yeliukhin@student.csn.khai.edu

Землянко Георгій Андрійович, асистент кафедри комп’ютерних систем, мереж і кібербезпеки. g.zemlynko@csn.khai.edu