Секція 2

ФУНКЦІОНАЛЬНА БЕЗПЕЧНІСТЬ СЕРВЕРІВ В КРИТИЧНІЙ ІНФРАСТРУКТУРІ

Кириченко Д. С.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г. А.

Актуальність. В нинішньому світі безперебійна робота ряду високотехнологічних служб та сервісів є життєво необхідною. Захист критичної інфраструктури є важливою проблемою усіх країн. Високий рівень розвитку сучасного суспільства залежить від багатьох послуг, в значній мірі наданих приватним бізнесом. До критичної інфраструктури відносяться об'єкти, мережі, служби та системи, збій в роботі яких позначиться на здоров'ї, безпеці і добробуті громадян країни [1]. Як приклади життєво важливої матеріальної інфраструктури можна виділити мости та дороги, аеропорти, електростанції, споруди зв'язку та воєнні бази. Ці та інші види інфраструктури неможливі без комп'ютерів, серверів та мереж, представлених системами диспетчерського керування і збору даних (SCADA) [2]. За останні роки відбувся ряд атак на критичні інфраструктури, такі як трагедія 11 вересня в США та 11 березня в Мадриді, які стали поворотним пунктом в глобальній безпеці та чітко зазначили необхідність мати стратегію уникнення потенціальних загроз. Як приклад – "The European for Critical Infrastructure Protection" [1].

Метою даної роботи є виявлення загроз та вразливостей на системах критичної інфраструктури.

Основні положення. Провівши аналіз відомих атак на кіберфізичні системи, були виявлені основні загрози та найбільші вразливості критичної інфраструктури [3]. Більшість атак на інформаційну інфраструктуру відбувається віддалено. Ці атаки використовують вразливості програмного коду на підприємстві. Головні серед вразливостей – застарілі та більш вразливі системи. Приватні та державні підприємства на яких відсутні належні практики оновлення систем безпеки стають найбільш частою ціллю хакерів. Також в звітах піднімаються питання контролю над обліковими записами, такі як обмеження доступу співробітників лише до тих функцій, які необхідні їм для роботи, та видалення облікових записів після звільнення працівника. Так, за останні пів року у Європі було чотири випадки, коли звільнені працівники мали доступ до облікового запису

систем управління, наприклад – загальний аккаунт GoToMyPC використовувався для видаленого доступу до систем у позаробочий час. При атаці на державні системи, такі як залізні дороги та аеропорти, хакери використовують цілий ряд вразливостей – від можливості встановити шкідливе програмне забезпечення та злом облікових записів до халатності або низькій кваліфікації працівників [4].

Висновки. Підприємства критичної інфраструктури насьогодні мають плани та рішення стосовно забезпечення інформаційної безпеки. Використовується фізична ізоляція сервера у закритому приміщення під охороною, використання автентифікації по ключам SSH, використання технологій VPN та SSL та своєчасне оновлення програмного забезпечення. Якщо та хакерські атаки не знаходять вразливостей, необхідно проводити моніторинг вторгнень до системи для своєчасного вияву вразливостей. Звісно не тільки шкідливе ПО та хакерські атаки можуть бути загрозою системам критичної інфраструктури. Так, поломки зі сторони апаратної частини системи внаслідок несвоєчасної фізичної профілактики та заміну термопасти, пилу, зносу елементів та фізичного втручання є загрозою працездатності системи на рівні втручання сторонньої особи в систему [5].

Список літератури

1. Критична інфраструктура. *Panda Security*. URL: https://mont.com/Content/files/pad_pad360%20-%20whitepaper%20-%20критические%20инфраструктуры.pdf (дата звернення: 19.11.2021);
2. Захист критично важливої інфраструктури. *McAfee Enterprise*. URL: https://www.mcafee.com/enterprise/ru-ru/about/public-policy/critical-infrastructure.html (дата звернення: 19.11.2021);
3. Software and systems engineering — Capabilities of software safety and security verification. *Online Browsing Platform.* URL – https://www.iso.org/obp/ui/#iso:std:iso-iec:23643:ed -1:v1:en (дата звернення: 21.11.2021);
4. Віддалена атака на сервер компанії водопостачання. *SecurityLab*. URL: https://www.securitylab.ru/news/526494.php (дата звернення: 20.11.2021);
5. Захист сервера від зламу URL: https://integrus.ru/blog/zashhita-servera-ot-vzloma.html (дата звернення: 21.11.2021).

Відомості про авторів

Кириченко Дмитро Сергійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 073-325-95-06, d.kirichenko@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu