УДК 004.056
Д. Урбан
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ЗАГРОЗ КОМП'ЮТЕРНИХ СИСТЕМ

UDC 004.056
D. Urban

ANALYSIS OF COMPUTER SYSTEM THREATS

Уразливість нульового дня – це слабке місце в комп'ютерній системі, яким може скористатися зловмисник і яке не помічають уражені сторони. Атака нульового дня – це спроба загрози проникнути, пошкодити або іншим чином скомпрометувати систему, уражену невідомою вразливістю. За характером нападу жертва не матиме засобів захисту, тому ймовірність успіху є високою.

Професіонали з IT-безпеки ще ніколи не стикалися з такими загрозами, чи то від величезного зростання віддаленої роботи, чи від агресивних хакерів, спонсорованих національною державою, таких як ті, хто причетний до зламу SolarWinds. Незважаючи на те, що завжди знайдуться нові діри, які потрібно закрити, уразливості системи безпеки зазвичай виникають через кілька тих самих причин: невиправлені вразливості, неправильні конфігурації чи помилки користувача, і навіть найбільш технічно підковані компанії вразливі до цих помилок.

Оскільки комп'ютери та інші цифрові пристрої стали важливими для бізнесу та торгівлі, вони також дедалі частіше стають об'єктами атак. Для того, щоб компанія чи окрема особа могли впевнено використовувати комп'ютерний пристрій, вони спочатку повинні бути впевнені, що пристрій жодним чином не скомпрометовано та що всі комунікації будуть безпечними.[1]

Кіберфізичні системи систем (SoSs) – це великомасштабні системи, створені з незалежних і автономних кіберфізичних складових систем (КС), які можуть взаємодіяти для досягнення цілей високого рівня також за втручання людей. Забезпечення безпеки в таких SoSs означає, серед інших функцій, прогнозування та передбачення розвитку функціональних можливостей SoSs, зрештою виявлення можливих шкідливих явищ, які можуть виникнути в результаті взаємодії КС та людей. Такі явища, які зазвичай називають емерджентними явищами, часто є складними і їх важко зафіксувати: перша поява емерджентного явища в кіберфізичному SoSs часто є несподіванкою для спостерігачів. Адекватна підтримка для розуміння явища, що виникає, допоможе зменшити як ймовірність проектних або експлуатаційних недоліків, так і час, необхідний для аналізу відносин між КС, що завжди має ключове економічне значення. Проте не варто вважати, що використання IDS та автоматизація аналізу log-файлів дозволить виявити всі загрози безпеки. Кожен засіб захисту адресовано конкретній загрозі безпеки в системі. Більше того, кожен засіб захисту має слабкі та сильні сторони. Тільки правильно підібравши та налаштувавши ці засоби, можна захиститися від максимально великого спектру атак. [2]

Література

1. Security of Cyber-Physical Systems. URL: https://www.powermag.com/security-of-cyber-physical-systems/.
2. What is a Zero-Day Exploit? URL: https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/what-is-a-zero-day-exploit.html.