УДК 004.056.5:004.75:004.8

Дмитрук Б. О., здобувач,
Ящук В.І., к.екон.н., доцент,
Ткаченко А.М., викладач
Львівський державний університет безпеки життєдіяльності

КОМПЛЕКСНИЙ АНАЛІЗ ВЕКТОРІВ ІНФІКУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ШКІДЛИВИМ ПРОГРАМНИМ КОДОМ ТА РОЗРОБЛЕННЯ БАГАТОРІВНЕВОЇ СТРАТЕГІЇ КІБЕРЗАХИСТУ

Шкідливий програмний код залишається одним з найпоширеніших та найбільш руйнівних засобів реалізації кібератак, спрямованих на порушення конфіденційності, цілісності й доступності інформаційних систем. Його проникнення здійснюється через широкий спектр векторів, що охоплюють як технічні, так і соціоінженерні методи. Комплексний аналіз таких векторів є необхідною передумовою для створення ефективної стратегії кіберзахисту сучасних цифрових інфраструктур.

До ключових векторів інфікування належать соціотехнічні атаки (phishing, spear-phishing, smishing), що базуються на використанні психологічних маніпуляцій для примушування користувачів виконати шкідливі дії; експлуатація вразливостей ПЗ та обладнання, включно з помилками в бібліотеках, драйверах, протоколах та некоректними конфігураціями серверів; компрометація ланцюгів поставок (supply chain attacks), зокрема у процесі оновлення програмного забезпечення, драйверів та контейнеризованих застосунків; використання незахищених мережевих сегментів, зокрема відкритих портів, хибно налаштованих VPN, незашифрованих протоколів взаємодії; зловживання легітимними інструментами системи (living-off-the-land techniques), коли зловмисники застосовують штатні утиліти, такі як PowerShell, WMI чи PsExec, мінімізуючи сліди активності.

У сучасних умовах класичні засоби антивірусного захисту часто виявляються недостатніми, оскільки шкідливий код дедалі частіше використовує поліморфізм, обфускацію, ін’єкції в пам’ять та безфайлові механізми. Це зумовлює необхідність переходу до багаторівневих систем захисту, що здатні реагувати не лише на відомі сигнатури, а й на поведінкові аномалії.

На рис. 1 - наведена пропонована багаторівнева стратегія кіберзахисту.

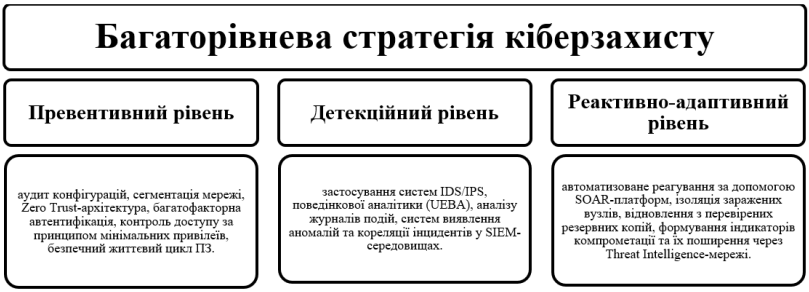

Рисунок 1 – Багаторівнева стратегія кіберзахисту

Особлива увага приділяється взаємодії між рівнями безпеки, що забезпечує стійкість системи до багатовекторних атак. Комбінація машинного навчання, аналізу поведінкових патернів і Zero Trust-підходу дозволяє мінімізувати площу атаки, обмежити рух шкідливого коду та забезпечити своєчасне виявлення навіть обфускованих або безфайлових загроз.

Комплексний аналіз векторів інфікування інформаційних систем демонструє, що сучасні атаки набувають багатокомпонентного та прихованого характеру. Ефективна протидія можливе лише за умов упровадження багаторівневого, адаптивного та проактивного кіберзахисту, що поєднує технологічні, поведінкові та політико-організаційні механізми. Запропонована стратегія дає змогу швидко виявляти шкідливий код, локалізувати наслідки інцидентів та підвищувати стійкість критично важливих цифрових інфраструктур до атак нового покоління.

Список використаних джерел:

1. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations : NIST Special Publication 800-53. Gaithersburg : NIST, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2. National Institute of Standards and Technology. Zero Trust Architecture : NIST Special Publication 800-207. Gaithersburg : NIST, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final

3. MITRE Corporation. MITRE ATT&CK Framework : Adversarial Tactics, Techniques, and Common Knowledge. McLean : MITRE, 2023. URL: https://attack.mitre.org

4. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2023. Athens : ENISA, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023