Petro Davydov

Рев’ю на тему

«ДОСЛІДЖЕННЯ ПЕРЕВАГ ЗАСТОСУВАННЯ МЕТОДУ ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ АУДИТУ З КІБЕРБЕЗПЕКИ ДЛЯ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ З ВИКОРИСТАННЯМ ВІРУСІВ-ВИМАГАЧІВ»

Вступ

У публікації, підготовленій колективом авторів - Дудикевичем В.Б, Гарасимчуком О.І, Партикою А.І, Совиним Я.Р, Нємковою О.А - розглядається актуальна проблема кібербезпеки в контексті захисту критичної інфраструктури України від атак вірусів-вимагачів (ransomware). Автори статті викладачі, доктори, доценти та професори кафедри захисту інформації та безпеки інформаційних технологій Національного університету «Львівська політехніка».

Основна тема дослідження - вивчення переваг перехресного впровадження міжнародних стандартів аудиту з кібербезпеки (*ISO 27001, PCI DSS, NIST*) як інструменту протидії кібер злочинам, зокрема атакам з використанням вірусів-вимагачів. Метою роботи є аналіз резонансних атак на критичну інфраструктуру України, розробка практичних рекомендацій для захисту бізнесу та державних установ, а також обґрунтування ефективності системного підходу до аудиту кібербезпеки.

Методологія

У статті використано описовий та аналітичний підхід до дослідження. Автори здійснили ретроспективний аналіз кібератак, що мали місце в Україні з 2015 по 2023 роки, зокрема інцидентів, пов’язаних із *BlackEnergy, Petya, BadRabbit, HermeticWiper, RemcosRAT* та *QuasarRAT*. Джерелами даних стали офіційні звіти Держспецзв’язку, CERT-UA, СБУ, а також публікації міжнародних організацій, таких як World Economic Forum.

Методи збору даних включали аналіз відкритих джерел, хронологічне структурування інцидентів**,** класифікацію типів атак та вивчення технічних характеристик шкідливого ПЗ. Також автори наводять кількісні показники, такі

як кількість атак, обсяг недовідпущеної електроенергії, кількість постраждалих користувачів, що дозволяє оцінити масштаб загроз.

Результати

Автори описують хвилі атак на українську критичну інфраструктуру:

- *Атака на енергосистему у 2015 - 2016 роках* з використанням *BlackEnergy* та *KillDisk*, що призвела до відключення електроенергії для сотень тисяч громадян.
- *Атака Petya у 2017 році*, яка поширювалася через легітимне ПЗ M.E.Doc і мала ознаки саботажу.
- *Хвиля псевдозамінувань у 2018 - 2019 роках*, що поєднувала технічні та інформаційні методи впливу.
- *Кібератаки 2022 - 2023 років*, синхронізовані з ракетними ударами, з використанням *HermeticWiper, Armageddon, Infamous Chisel, RemcosRAT*.

Усі ці інциденти демонструють *зростаючу складність атак, використання соціальної інженерії, бекдорів, інструментів горизонтального поширення* (EternalBlue, Mimikatz, PsExec), а також *цілеспрямованість на об'єкти енергетики, зв'язку, логістики та державного управління.*

Автори статті наголошують на тому, що *перехресне впровадження стандартів аудиту* дозволяє:

- Виявляти слабкі місця в інфраструктурі.
- Підвищувати рівень готовності до інцидентів.
- Забезпечувати відповідність законодавству.
- Формувати культуру кібербезпеки серед персоналу.

Ключові інсайти

1. *Інтеграція стандартів*

Поєднання ISO 27001, PCI DSS і NIST дозволяє охопити всі рівні захисту - від політик до технічних контролів. Це важливо для побудови системи, яка не лише реагує, а й запобігає атакам.

Пояснення: Сертифікація яку проходять підприємства не є формальністю (хоча і тут можна посперечатись) - це інструмент підтверджуючий знання в якості методів та способів захисту. Це варто врахувати при побудові систем SIEM.

2. *Легітимне ПЗ як вектор атаки*

Атака через M.E.Doc показує, що навіть довірені системи можуть бути використані для поширення шкідливого ПЗ.

Пояснення: Треба звертати увагу на політику оновлень, контроль змін системах, Приділити увагу процедурам пов'язаним з роботою DevSecOps.

3. *Синхронізація кібератак з фізичними ударами*

Атаки 2022 року демонструють, що кіберзагрози можуть бути частиною гібридної війни.

Пояснення: В наш час кібератаки - це невід'ємна частина військових операцій, що ми можемо спостерігати. І хоча є думка певних посадовців що «кібербезпека в Україні переоцінена», ми бачимо, що, це частина «гібридних війн». Це треба враховувати при *моделюванні загроз* у критичних системах.

4. *Недостатність одного рівня захисту*

Окремі заходи захисту вже не гарантують безпеки, як це було на початку розвитку ери інтернету. Потрібна багаторівнева система захисту.

Пояснення*:* Треба звернути увагу на такі поняття як "layered security" та "defense-in-depth" (дивитись у словнику).

5. *Роль людського фактора*

Це найбільша проблема у всі часи. Тому без навчання персоналу, хоча б мінімальним знання зі сфери кібербезпеки (принаймні кібергігієні) ми наражаєм себе на небезпеку. Фішинг та соціальна інженерія - вектори атак, які існували і продовжують існувати з часу бажання людини дістати «безкоштовний сир з мишоловки».

Пояснення: «Люди + тренінги з кібергігієни», як мінімум, мають бути включені у будь яку стратегію розробки кібербезпеки.

Інструменти які могли були використані на різних етах атаки

1. *Розвідка*

* збір інформації про ціль, її інфраструктуру, відкриті порти, служби, домени, облікові записи.

Інструмент	Призначення
Nmap	Сканування портів, виявлення служб, ОС, версій - наприклад, на енергосистемах
Gobuster	Перебір директорій і файлів на вебсерверах - корисно для дефейс атак
WhatWeb	Ідентифікація технологій вебзастосунку (CMS, фреймворки)
Enum4linux	Збір інформації з Windows серверів (SMB, NetBIOS, домени)
Wireshark	Аналіз мережевого трафіку - виявлення незашифрованих протоколів

2. *Експлуатація (Initial access & Exploitation)*

* ціль - отримати доступ до системи через вразливості, слабкі паролі або фішинг.

Інструмент	Призначення
Hydra	Брутфорс паролів на службах (SSH, FTP, RDP)
Burp Suite / ZAP Proxy	Перехоплення HTTP запитів, виявлення XSS, SQLi, CSRF, фішинг-форм
Mimikatz	Експлуатація Windows для отримання облікових даних (паролі, хеші)
John the Ripper / Hashcat	Злам хешів паролів, отриманих через Mimikatz або витоки

3. *Рух у мережі (Privilege Escalation & Lateral Movement)*

* поширення в мережі, підвищення прав, захоплення критичних вузлів.

Інструмент	Призначення
PsExec / WMIC	Горизонтальне поширення в мережі (як у випадку з Petya)
Mimikatz	Повторне використання для отримання токенів, SID, прав адміністратора
Netcat	Встановлення зворотного шелу, тунелювання команд

4. *Приховування слідів та постексплуатація (Persistence & Cleanup)*

* ціль - зберегти доступ, приховати сліди, ексфільтрувати дані.

Інструмент	Призначення
CyberChef	Декодування, шифрування, обфускація даних перед ексфільтрацією
GPG / OpenSSL	Шифрування файлів перед передачею або зберіганням
Wireshark	Перевірка, чи не залишено незашифрованих слідів у трафіку
Netcat	Виведення даних через нестандартні порти, приховані канали

Висновок

Публікація є важливим внеском у розуміння сучасних кіберзагроз, зокрема атак вірусів-вимагачів, які стали частиною гібридної війни проти України та внесли свій вклад у всі війни на планеті. Автори не лише систематизували хронологію атак, а й запропонували практичні рекомендації для захисту бізнесу та державних структур.

Проаналізувавши роботу можемо зауважити, що автори зробили обґрунтування ефективності *перехресного впровадження стандартів аудиту*, що дозволяє створити *стійку, адаптивну систему кіберзахисту*. Це треба практикувати та застосовувати на практиці, як технічному фахівцю та спеціалісту з кібербезпеки.

Перспективи подальших досліджень можуть включати:

- Розробку національного фреймворку кібербезпеки (interesting, but why not).
- Вивчення ефективності SIEM-систем у ранньому виявленні атак.
- Аналіз впливу людського фактору на успішність впровадження стандартів.

Словник

Стандарти та фреймворки

ISO 27001 - міжнародний стандарт управління інформаційною безпекою, що визначає вимоги до побудови, впровадження та підтримки ISMS (системи управління безпекою).

PCI DSS - стандарт безпеки даних платіжних карток, обов'язковий для організацій, що обробляють, зберігають або передають дані карток.

NIST (800-53 / CSF) - набір рекомендацій від Національного інституту стандартів США щодо кібербезпеки, управління ризиками та реагування на інциденти.

Віруси-вимагачі та шкідливе ПЗ

BlackEnergy - троян, що використовувався для атак на енергетичну інфраструктуру України; дозволяв віддалене управління та виконував деструктивні дії.

Petya - шкідлива програма, яка шифрувала MBR (головний завантажувальний запис) і дані, поширювалася через оновлення M.E.Doc.

BadRabbit - вірус-вимагач, що маскувався під оновлення Adobe Flash; використовував техніки lateral movement.

HermeticWiper - шкідливе ПЗ для знищення даних, активне під час початку повномасштабного вторгнення в Україну.

RemcosRAT - віддалений троян-адміністратор, що дозволяє повний контроль над зараженим пристроєм.

QuasarRAT - легкий RAT з відкритим кодом, який використовується для шпигунства та збору даних.

KillDisk - утиліта, що стирає дані на диску, використовувалась у зв'язці з BlackEnergy для знищення інформації.

Armageddon - російське хакерське угруповання, що спеціалізується на кібершпигунстві проти українських сил безпеки.

Infamous Chisel - шкідливе ПЗ для Android, яке використовувалось для стеження за мобільними пристроями військових.

Інструменти атак

EternalBlue - експлойт у протоколі SMBv1, який дозволяє несанкціонований доступ до системи; використовувався у Petya.

Mimikatz - інструмент для вилучення облікових даних з пам’яті Windows, зокрема паролів та хешів.

PsExec - утиліта для віддаленого виконання команд у Windows, часто використовується для lateral movement.

Атаки та інфраструктура

Атака через M.E.Doc - кібератака, в якій легітимне бухгалтерське ПЗ використовувалось для поширення вірусу Petya.

M.E.Doc - українське програмне забезпечення для електронної звітності, яке стало вектором атаки у 2017 році.

CERT-UA - урядова команда реагування на комп’ютерні інциденти в Україні, що координує кіберзахист державних структур.

Концепції безпеки

Layered security - концепція багаторівневого захисту, де кожен рівень (мережа, пристрій, користувач) має власні механізми безпеки.

Defense-in-depth - стратегія, що передбачає використання кількох незалежних засобів захисту для зменшення ризику успішної атаки.