МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Захист інформації в спеціалізованих ІТС

Практичне заняття №3

Дослідження кіберзагроз та вразливостей в спеціалізованих ІТС на прикладі кіберінцидентів в промисловості

Перевірив:
Зубок В. Ю.

Виконав:
студент І курсу
групи ФБ-41мп
Сахній Н. Р.

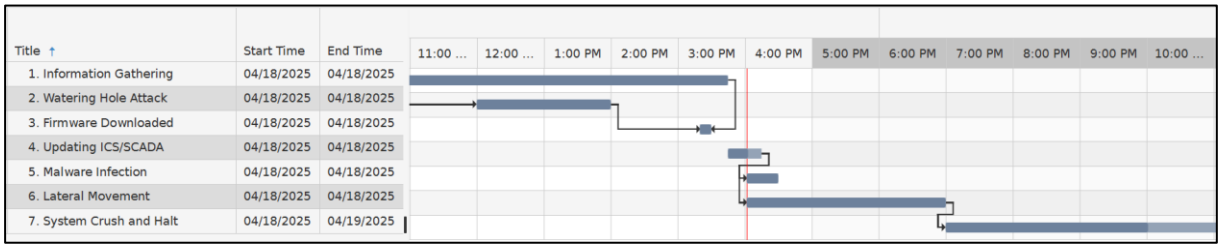
Київ 2025

Завдання (№3. Зараження ШПЗ)**:** За матеріалами розділу 5 із документу «Communication network dependencies for ICS/SCADA Systems» провести аналіз наведеного сценарію кібератаки на комунікаційні мережі в ICS.

За результатами аналізу відобразити та навести пояснення про:

- Типовий сценарій атаки у вигляді часової діаграми Ганта

1) Збір інформації зловмисником про ресурси, з яких завантажуються оновлення.
2) Проведення “Watering Hole”-атаки на цільові ресурси.
3) Завантаження оператором інфікованого файлу з ресурсу на свою робочу станцію, яка використовується для з’єднання з ICS/SCADA-пристроями.
4) Встановлення інфікованої версії оновлення на пристроях ICS/SCADA.
5) Інфікування шкідливим ПЗ пристроїв ICS/SCADA.
6) Поширення зразків шкідливого ПЗ по всій мережі.
7) Збій процесів усієї системи та повна зупинка її роботи.



- Ступінь впливу атаки

Critical: Під час проведення технічного обслуговування з’єднання зазвичай здійснюється безпосередньо з системами SCADA (локально або через VPN), що створює потенційно вразливу точку доступу, адже у разі її використання зловмисником будь-яка компрометація, маніпулювання або переривання в роботі систем SCADA може вплинути на багатьох людей або навіть спричинити проблеми з навколишнім середовищем.

Пояснення: Загалом, інфікування ШПЗ може мати значний вплив на виробничий процес, адже можливе порушення роботи обладнання, аж до повної зупинки роботи об’єкту.

➢ Складність виявлення атаки

Easy/Medium: Виявлення значною мірою буде залежати від вжитих заходів безпеки, оскільки це визначатиме ймовірність виявлення. Периметральні заходи безпеки мережі (н/д, антивірус або IDS) ймовірно, що зможуть виявити ці загрози.

Пояснення: Насправді, складність виявлення залежить від наявності відповідних систем захисту. Адже, для прикладу, при наявності в інфраструктурі перевіреного антивірусу або надійної IDS-системи – виявити ШПЗ, по суті, буде досить просто.

➢ Ризик каскадного ефекту

Low/Medium: Операції з технічного обслуговування зазвичай проводяться всередині компанії, підключаючись безпосередньо до систем й оминаючи інтранет та локально впроваджені заходи безпеки. Це призводить до ризику зараження внутрішніх систем і сприяє їх розширенню, що потенційно може поширитися на інші середовища та сектори.

Пояснення: Фактично, ризик каскадного ефекту залежить від ступеню інтегрованості зараженої системи з іншими системами. При зараженні однієї системи є ймовірність поширення шкідливого ШПЗ на інші, пов’язані з цією, внутрішні системи.

➢ Які активи виробничого процесу вражаються?

- **SCADA assets** – можуть бути заражені під час оновлення, що призведе до втрати керування, помилкових команд або повного виходу системи з ладу.
- **Data Historian** – можливе викрадення або модифікація історичних даних, із метою приховування слідів атаки або компрометації аналітичних процесів.
- **HMI** (Human Machine Interfaces) – може відображати некоректну інформацію, вводити оператора в оману щодо реального стану або блокувати керування.
- **PLCs** (Programmable Logic Controllers) – можливе перепрограмування або пошкодження логічних контролерів, що тим самим може призвести до небезпечних змін у виробничих процесах або навіть фізичних пошкоджень.

- Запобіжні заходи, що зменшують ймовірність та/або успішність атаки
  - ✓ Сегрегація мережі залежно від призначення для обмеження поверхні атаки.
  - ✓ Ізоляція сегментів мережі КІ для запобігання поширенню шкідливого ПЗ.
  - ✓ Використання “традиційних” засобів захисту периметру та мережі: фаєрвол, антивірус, системи виявлення/запобігання вторгнень (IDS/IPS).
  - ✓ Ізоляція систем, що перебувають на технічному обслуговуванні (оновленні), для запобігання випадковому інфікуванню шкідливим ПЗ.
  - ✓ Використання для оновлень лише виділених систем на комп’ютерів, щоб уникнути зараження через системи/пристрої загального призначення.
  - ✓ Увімкнення віддаленого доступу лише на необхідний внутрішнім персоналом.
  - ✓ Періодичний аналіз ризиків системи для оцінки потенційних вразливостей.
  - ✓ Управління конфігурацією всіх систем для швидкого виявлення відхилень.
  - ✓ Моніторинг логів для виявлення аномальних/неочікуваних з’єднань/трафіку.