Модуль 4. Основи хакінгу та розслідування інцидентів в ISC/SCADA системах

Лекція 1: Загрози, вразливості та вектори атак в ICS/SCADA

Мета лекції

Сформувати цілісне розуміння загроз, вразливостей і векторів атак проти ICS/SCADA, а також практичних підходів до їх попередження та розслідування.

Основні завдання

Типи противників
Розрізняти типи противників та їх мотивацію: державні суб'єкти, кіберзлочинці, інсайдери, хактивісти.

Типові вразливості
Визначати типові вразливості COTS-ПЗ, ОС, баз даних, веб-інтерфейсів і протоколів ОТ; розуміти роль hardening.

Вектори атак
Класифікувати вектори атак: фізичний доступ, електронний доступ через мережі, знімні носії, підключення до корпоративної WAN.

Багаторівневий захист
Вибудовувати багаторівневий захист: сегментація, DMZ, контроль віддаленого доступу, політики щодо носіїв та портативних пристроїв.

Протидія соціальній інженерії
Протидіяти соціальній інженерії через навчання персоналу, MFA, контроль процесів і підвищення обізнаності.

Основи інцидент-розслідування
Закласти основу для інцидент-розслідування: інвентар активів, журналювання, політики доступу та процедурні вимоги.

1.1. Поширені загрози (державні суб'єкти, кіберзлочинці, інсайдери, хактивісти)

1.1.1. Поширені загрози в ICS/SCADA системах

Державні суб'єкти

Найнебезпечніші зловмисники з значними ресурсами та високою мотивацією. Розробляють складні інструменти для економічного збитку, шпигунства та саботажу критичної інфраструктури.

Кіберзлочинці

Мотивовані фінансовою вигодою групи, що використовують ransomware та шкідливі програми для вимагання коштів. Приклад - атака на Colonial Pipeline у 2021 році.

Інсайдери

Загрози від співробітників можуть бути навмисними чи ненавмисними. Мають безпосередній доступ до систем та можуть обійти фізичні й електронні заходи безпеки.

Хактивісти

Мотивовані ідеологічними, політичними або соціальними причинами. Атакують системи для привернення уваги до своїх цілей та викликання суспільного резонансу.

1.1.2. Державні суб'єкти: найпотужніша загроза

Характеристики державних акторів

- Значні фінансові та технічні ресурси
- Високорозвинені навички та інструменти
- Довгострокові стратегічні цілі
- Здатність до складних кібер-фізичних атак

Приклад Stuxnet - атака на ядерну програму Ірану через маніпуляцію ПЛК, що керували центрифугами, демонструє потужність державних суб'єктів.

За даними Всесвітнього економічного форуму 2019 року, кібератаки займають 4-ту та 5-ту позиції серед глобальних ризиків.

1.1.3. Фінансово мотивовані кіберзлочинці

$52M

Втрати Norsk Hydro

Збитки від LockerGoga лише за перший квартал 2019 року

$1B+

WannaCry та Petya

Сукупні збитки від цих атак склали мільярди доларів

Кіберзлочинці використовують програми-вимагачі та інші шкідливі програми для вимагання коштів. Атака на Colonial Pipeline у 2021 році призвела до значних порушень постачання палива в США, демонструючи вразливість критичної інфраструктури до фінансово мотивованих атак.

1.1.4. Загроза від інсайдерів

1

Ненавмисні дії

Випадкове зараження систем через використання знімних носіїв або недбалість. Значна частина кіберінцидентів спричинена людським фактором.

2

Навмисні інсайдери

Незадоволені колишні співробітники можуть використовувати знання про систему для шкідливих атак, маючи доступ до документації та практичний досвід.

3

Обхід захисту

Інсайдери можуть обійти фізичні та електронні заходи безпеки, маючи безпосередній доступ до системи та розуміння її архітектури.

1.1.5. Еволюція ICS/SCADA систем

Минуле

Ізольовані системи з власними апаратними засобами та програмним забезпеченням. Менш схильні до кібератак через закритість.

1

Сьогодення

Зближення IT та OT технологій. SCADA-системи архітектурно ідентичні IT-системам, за винятком спеціалізованих додатків.

2

Виклики

Потреба в 100% доступності при збільшеній вразливості до традиційних IT-атак через використання COTS продуктів.

3

1.2. Вразливості у комерційних продуктах та операційних системах

1.2.1. Вразливості комерційного програмного забезпечення

Операційні системи

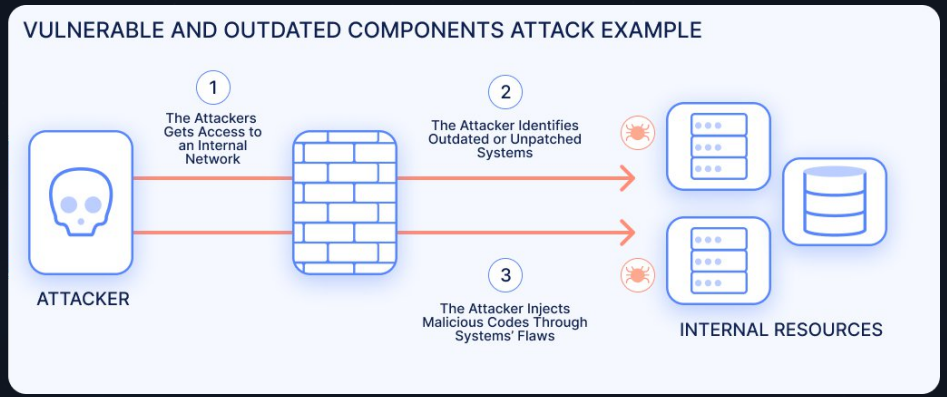
Більшість SCADA-систем працюють на платформах Intel x86 з Windows або Linux. Microsoft Windows часто постачається з "небезпечними" конфігураціями за замовчуванням.

Реляційні бази даних

Використання SQL Server, Oracle або OSI-PI як сховищ даних. Ці бази можуть мати вразливості, такі як SQL-ін'єкції для маніпуляції даними.

Веб-сервери

SCADA-системи надають операторський інтерфейс через веб-сервери на стандартних ПК. Веб-сервери відомі своїми численними вразливостями.



1.2.2. Проблеми застарілого ПЗ та протоколів

Застаріле програмне забезпечення

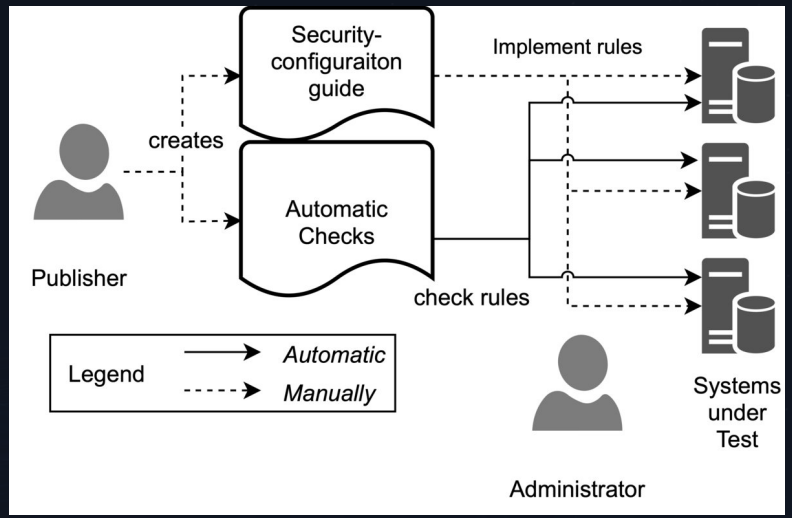
SCADA-системи часто залишаються на старих, незахищених версіях ПЗ/прошивок через складність оновлення. Це створює "бекдори" та інші вразливості. Відсутність своєчасного оновлення є однією з найпоширеніших проблем.

Небезпечні протоколи

Протоколи ICS/SCADA розроблялися в епоху закритих середовищ, коли безпека не була пріоритетом. Протоколи Modbus та KNX/IP не є безпечними та стійкими до кібератак.

⊗ Багато протоколів не захищають вміст повідомлень та не передбачають захисту від атак "людина посередині"

1.2.3. Недостатнє "загартовування" систем



01

Проблема

Заводські налаштування комерційних ОС часто незахищені та містять відомі вразливості. IT-відділи не проводять адекватне hardening систем.

02

Hardening процес

Видалення або відключення непотрібних служб, утиліт, інструментів та програм для мінімізації поверхні атаки.

03

Утиліти SCADA

Спеціалізовані утиліти для конфігурації та обслуговування також можуть бути вразливими, особливо якщо потрапляють до зловмисників.

1.3. Вектори атак (фізичний доступ, електронний доступ, знімні носії, підключення до корпоративної WAN)

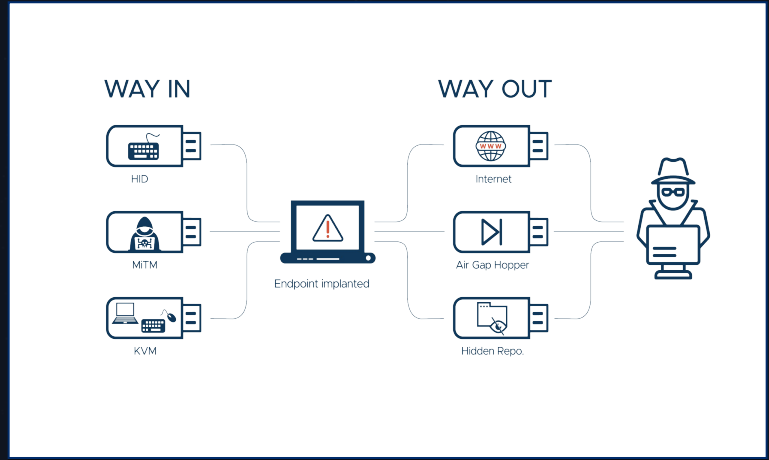
1.3.1. Вектори атак: фізичний доступ

Прямий доступ

Використання інтерфейсів (клавіатура/миша/дисплей) та периферійних пристроїв для запуску кібератаки при фізичному доступі до системи.

Обхід захисту

Фізичний доступ дозволяє обійти електронні та логічні засоби захисту, включаючи підключення шкідливих пристроїв.



Фізична безпека критичних елементів системи управління є одним з основних правил. Приклад Stuxnet показав успішність атаки навіть при фізичній ізоляції об'єкта від зовнішніх мереж, підкреслюючи важливість фізичної безпеки.

1.3.2. Електронний доступ через мережі

1 2 3

Корпоративна WAN

SCADA-системи підключаються до корпоративних мереж для обміну інформацією з бізнес-системами, створюючи шлях для атак.

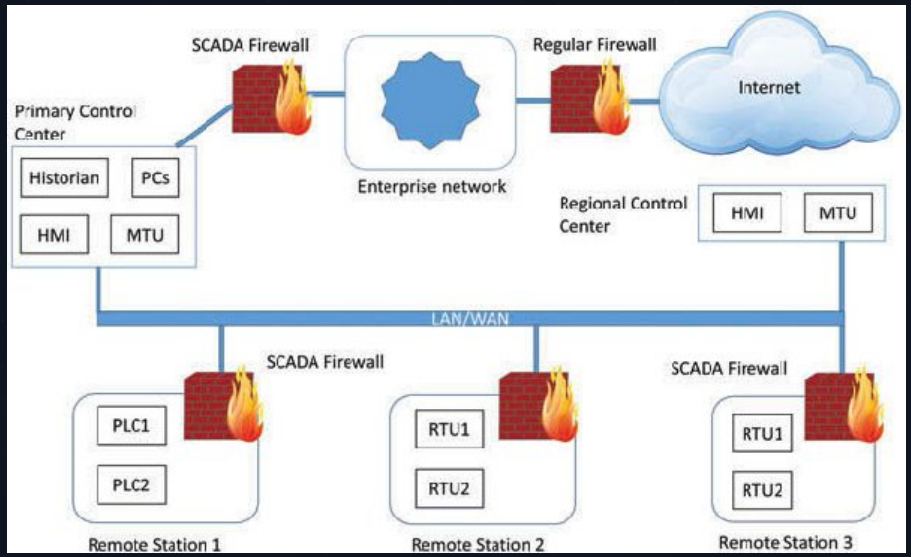
⚠ Експерти з кібербезпеки вважають, що SCADA-системи не повинні мати прямого доступу до Інтернету

Інтернет-з'єднання

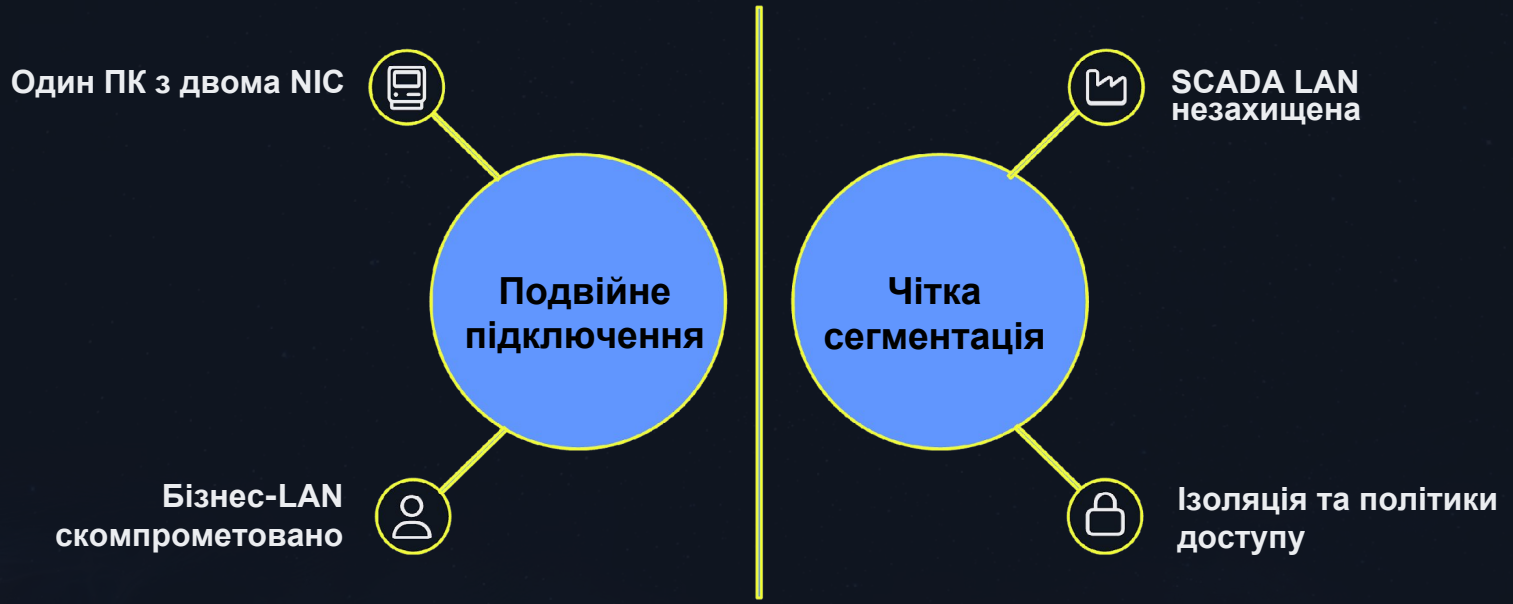
Корпоративні мережі часто підключені до Інтернету, створюючи прямий шлях для зовнішніх атак на SCADA-системи.

Компрометація

Зловмисники використовують телекомунікаційні з'єднання через LAN, WAN або телефонні мережі для віддаленого доступу.



1.3.3. Проблема подвійного підключення



Використання одного ПК з двома мережевими картами створює експлуатований шлях для атаки. Зловмисник, скомпрометувавши бізнес-ПК, отримує прямий доступ до SCADA-системи. Навіть вбудовані Wi-Fi та Bluetooth інтерфейси можуть створити міст між мережами.

1.3.4. Загроза знімних носіїв

USB-накопичувачі

Персонал може ненавмисно занести шкідливе ПЗ через USB-флешки, включаючи ті, що роздавалися на виставках.

Ноутбуки підрядників

Компрометовані ноутбуки підрядників можуть стати джерелом зараження при підключенні до робочих систем.

Мобільні телефони

Особисті мобільні телефони співробітників, підключені навіть для зарядки, можуть передати шкідливе ПЗ.

1.3.5. Контроль знімних носіїв

Необхідні заходи

- Впровадження процедур управління портативними носіями
- Контроль використання USB-пристроїв у виробничому середовищі
- Використання лише "довірених" носіїв
- Регулярне сканування на шкідливе ПЗ

В деяких галузях, таких як ядерна енергетика, застосовується практика використання лише попередньо перевірених та схвалених носіїв інформації.

Необхідно впроваджувати суворі політики щодо будь-яких портативних пристроїв, що підключаються до SCADA-систем

1.4. Соціальна інженерія (Social Engineering)

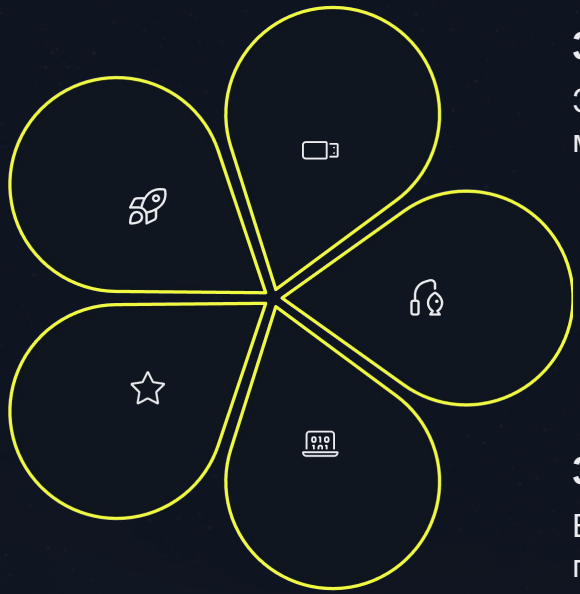
1.4.1. Соціальна інженерія: людський фактор

Маніпуляція довірою

Видавання себе за авторизований персонал для отримання доступу

Крадіжка облікових даних

Викрадення імен користувачів та паролів через маніпуляції



Заражені носії

Залишення USB-накопичувачів у місцях, де їх знайдуть співробітники

Фішинг атаки

Атаки на корпоративні мережі як плацдарм для проникнення в OT

Збір інформації

Використання OSINT для створення переконливих сценаріїв

1.4.2 Класичний сценарій соціальної інженерії

Підготовка

Зловмисник залишає заражені USB-накопичувачі на парковці або в офісі компанії, розраховуючи на цікавість співробітників.

Знаходження

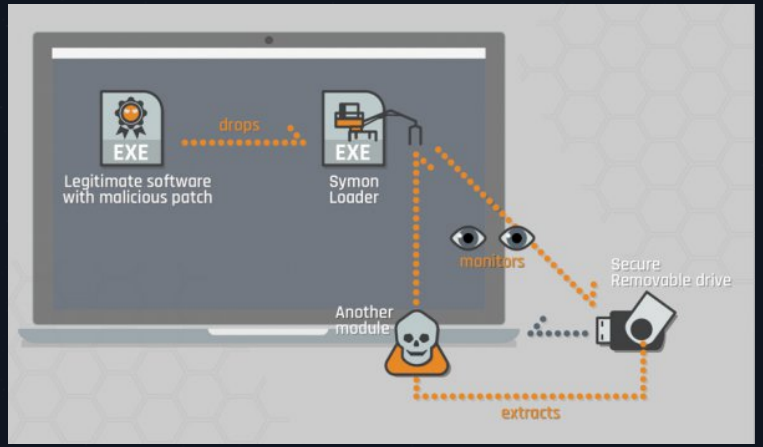
Співробітник знаходить накопичувач і з цікавості або намагаючись знайти власника, вирішує підключити його до робочої станції.

Зараження

При підключенні накопичувача автоматично запускається шкідливе ПЗ, яке заражає систему та може поширитися по мережі.

Компрометація

Зловмисник отримує доступ до системи та може використовувати його для подальшого проникнення в критичні системи управління.



1.4.3. OSINT та збір інформації

LinkedIn розвідка

Пошук посад співробітників, інформації про обладнання/ПЗ та структуру організації для створення переконливих атак.

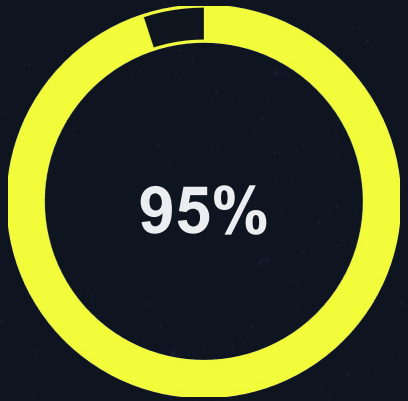
Витоки даних

Використання сервісів типу "Have I Been Pwned" та Dehashed для отримання скомпрометованих облікових даних.

Скрейпери електронних адрес

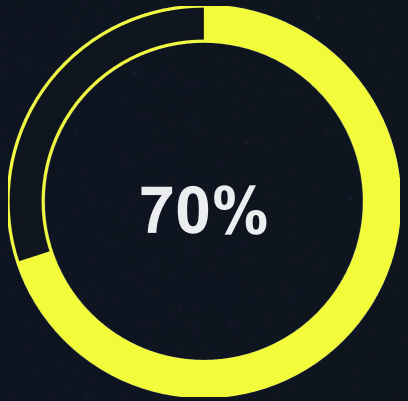
Автоматизований збір електронних адрес для подальших фішингових кампаній проти співробітників.

1.4.4. Статистика людського фактору



Кіберінциденти

Міжнародна статистика показує, що більшість кіберінцидентів спричинена людським фактором

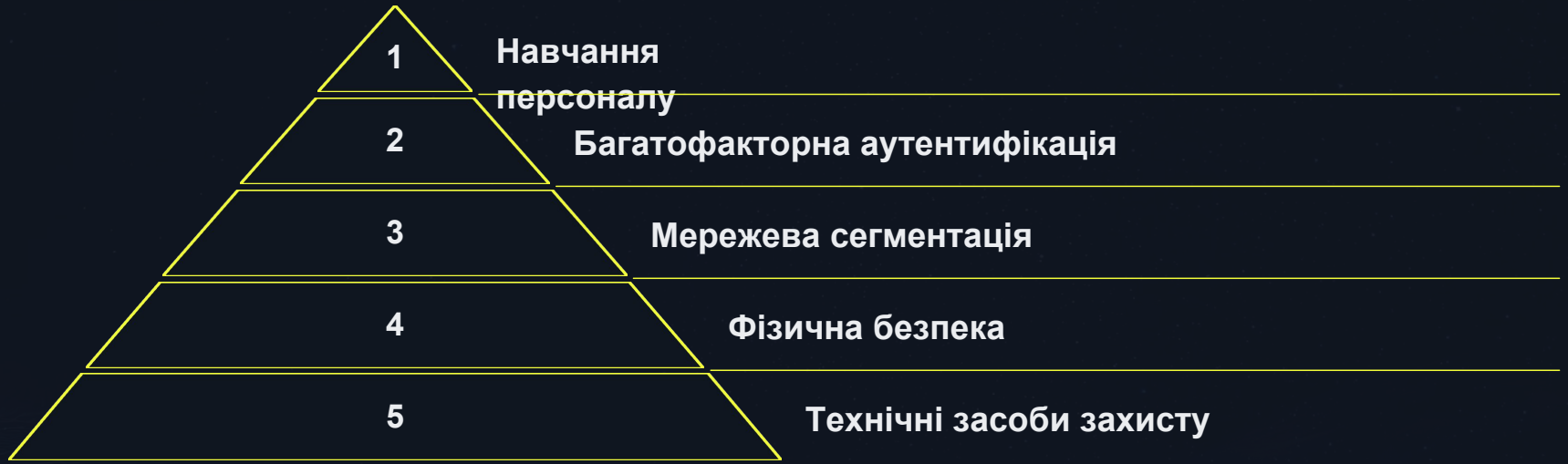


Успішність фішингу

Відсоток співробітників, які можуть стати жертвами добре підготовленої фішингової атаки

Соціальна інженерія є однією з найскладніших загроз, оскільки експлуатує людську природу, а не технічні вразливості. Навіть найсучасніші технічні засоби захисту можуть бути обійдені через маніпуляцію людьми.

1.4.5. Багаторівневий підхід до захисту



Ефективний захист ICS/SCADA систем вимагає комплексного підходу, що поєднує технічні, процедурні та організаційні заходи на всіх рівнях інфраструктури.

1.4.6. Рекомендації щодо захисту від соціальної інженерії

1

Навчання та обізнаність

Регулярне навчання персоналу щодо ризиків соціальної інженерії, фішингу та безпечного використання знімних носіїв. Оператори повинні розуміти зв'язок між кібер- та фізичними системами.

2

Політики щодо носіїв

Впровадження та дотримання суворих політик, які обмежують або контролюють використання USB-накопичувачів та інших портативних пристроїв у виробничому середовищі.

3

Багатофакторна аутентифікація

Використання MFA для доступу до критичних систем значно ускладнює зловмисникам використання викрадених облікових даних навіть при успішній соціальній інженерії.

1.4.7. Технічні рекомендації щодо загартовування

1 **Регулярне оновлення ПЗ**

Своєчасне оновлення програмного забезпечення та прошивок зменшує кількість відомих вразливостей та закриває потенційні шляхи для атак.

2 **Загартовування систем**

Видалення або відключення непотрібних служб, утиліт та функцій для мінімізації поверхні атаки та зменшення ризиків компрометації.

3 **Контроль доступу**

Впровадження суворих політик доступу, обмеження доступу до системних утиліт та конфігураційних файлів лише для авторизованого персоналу.

4 **Безпечні протоколи**

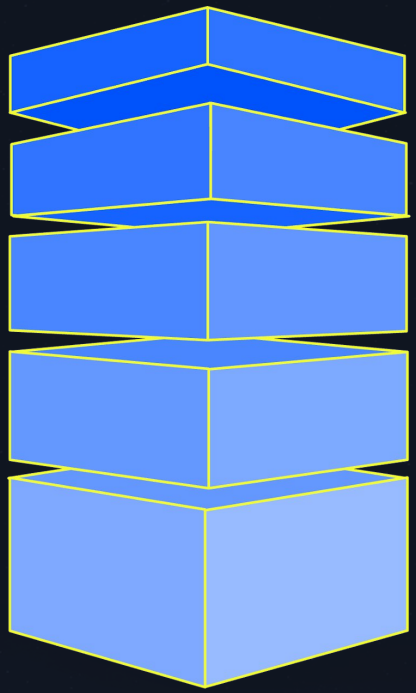
Використання захищених протоколів та механізмів шифрування/аутентифікації, заміна застарілих незахищених протоколів або впровадження додаткових рівнів захисту.

1.4.8. Мережева архітектура безпеки

Фундамент: Сегментація
Відокремити мережі SCADA і корпоративну.

Контроль доступу
Впровадити контрольовані точки доступу між сегментами.

Захисний периметр
Шари фаєрволів і IDS/IPS для захисту критичного.



Рівень DMZ
Розмістити сервера обміну через DMZ з фаєрволами.

Моніторинг трафіку
Постійний аналіз і логування між мережами.

Правильна мережева сегментація є критично важливою для захисту ICS/SCADA систем. Використання DMZ, фаєрволів та контрольованих точок доступу допомагає ізолювати критичні системи від потенційних загроз.

1.4.9. Моніторинг та виявлення загроз

Мережевий моніторинг

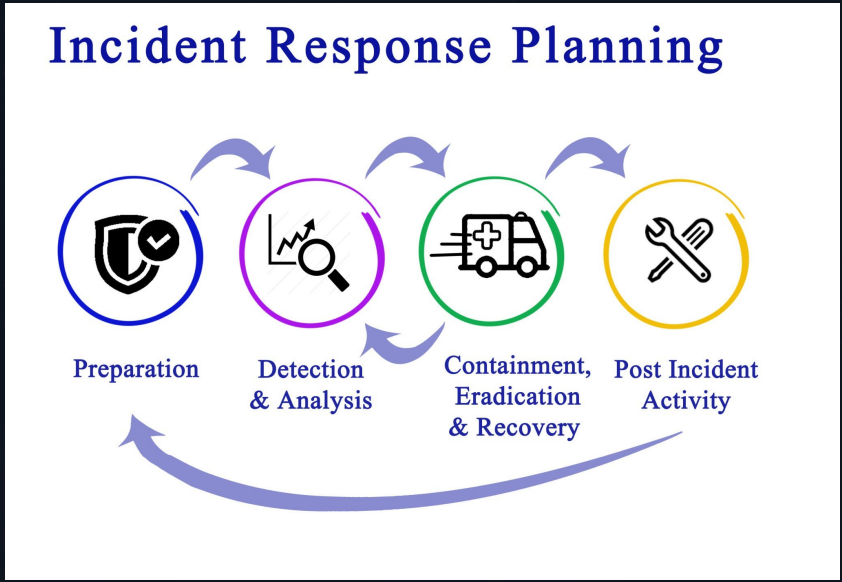
Постійний моніторинг мережевого трафіку для виявлення аномальної активності, несанкціонованих з'єднань та підозрілих комунікацій між системами.

Аналіз логів

Централізований збір та аналіз логів з усіх критичних систем для швидкого виявлення інцидентів безпеки та порушень політик доступу.

Реагування на інциденти

Розробка та впровадження процедур швидкого реагування на кіберінциденти, включаючи ізоляцію скомпрометованих систем та відновлення операцій.



1.4.10. Управління ризиками в ICS/SCADA

Оцінка ризиків

Регулярна оцінка кіберризиків та вразливостей

Політики безпеки

Розробка та впровадження комплексних політик кібербезпеки

Програми навчання

Постійне навчання персоналу основам кібербезпеки

Постійне вдосконалення

Регулярний перегляд та оновлення заходів безпеки

1.5. Висновки та майбутні виклики

Комплексний підхід

Кібербезпека в ICS/SCADA вимагає багаторівневого підходу, що поєднує технічні, процедурні та організаційні заходи для ефективного захисту критичної інфраструктури.

Людський фактор

Соціальна інженерія залишається однією з найефективніших загроз. Навчання персоналу та підвищення обізнаності є критично важливими для захисту систем.

Постійна пильність

Загроза кібератак залишатиметься актуальною. Необхідний постійний моніторинг, оновлення систем захисту та адаптація до нових викликів кібербезпеки.

Розуміння загроз, вразливостей та векторів атак є основою для побудови ефективної системи кібербезпеки промислових об'єктів. Лише комплексний підхід може забезпечити надійний захист критичної інфраструктури.

Список використаних джерел

1. Radvanovsky, R., & Brodsky, J. (2016). Handbook of SCADA/Control Systems Security (2nd ed.). CRC Press.

2. Colbert, E. J. M., & Kott, A. (Eds.). (2016). Cyber-Security of SCADA and Other Industrial Control Systems. Springer.

3. Shaw, W. T. (2020). Cybersecurity for SCADA Systems (2nd ed.). PennWell Books.

4. Brooks, C. J., & Craig Jr., P. A. (2022). Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT. Wiley.

5. Kouremetis, M. (2014). Defending a SCADA System with the Snort IDS [Presentation]. ECSSE Department.

6. National Telecom Regulatory Authority (NTRA). (2022). IoT Cyber Security Framework. EG-CERT.

7. Emerson. (2021). Industrial Security in SCADA Systems: IEC 62443-3-3 Certification. Emerson Automation Solutions.

8. Krotofil, M. (2023). Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle. Technical White Paper.

9. UtilSec, LLC. (2024). Getting Started in ICS/OT Cyber Security: Lab Manual. UtilSec.

Дякую за увагу!