Модуль 3. Основні принципи мережевого захисту для ICS/SCADA та інтеграції промислових систем в IT-інфраструктуру

Лекція 3: Фізична безпека в середовищах ICS/SCADA

Мета лекції

Сформувати розуміння ролі фізичної безпеки як невід'ємної частини загальної стратегії кіберзахисту ICS/SCADA.

Основні завдання:

Пояснити важливість фізичного доступу як критичного вектора загроз

Розглянути багаторівневі заходи контролю доступу (огорожі, замки, електронні системи)

Показати взаємозв'язок фізичних і кіберзасобів захисту

Ознайомити з принципами інтеграції фізичної та функціональної безпеки на основі стандартів (IEC 62443, IEC 61508)

Підкреслити роль персоналу, документації та інвентаризації для підтримки стійкості

3.1. Важливість фізичної безпеки для активів ICS/SCADA

3.1.1. Фізичний доступ як критична загроза

Фізична безпека є надзвичайно важливою для захисту систем промислового контролю (ICS/SCADA), оскільки фізичний доступ до SCADA-системи може бути навіть більш ефективним способом виведення її з ладу, ніж кібератака.

Роль фізичної безпеки полягає у виявленні, встановленні та підтримці передбачуваного та контрольованого середовища щодо управління діями або умовами, які можуть навмисно або ненавмисно завдати шкоди персоналу, активам та операціям організації.

3.1.2. Історичні виклики SCADA-систем

Традиційна залежність

Значна залежність від фізичних заходів безпеки через відносну відсутність інтеграції в рамках підприємства

Розподілена архітектура

Складність управління безпекою через географічно розподілені компоненти системи

Застарілі технології

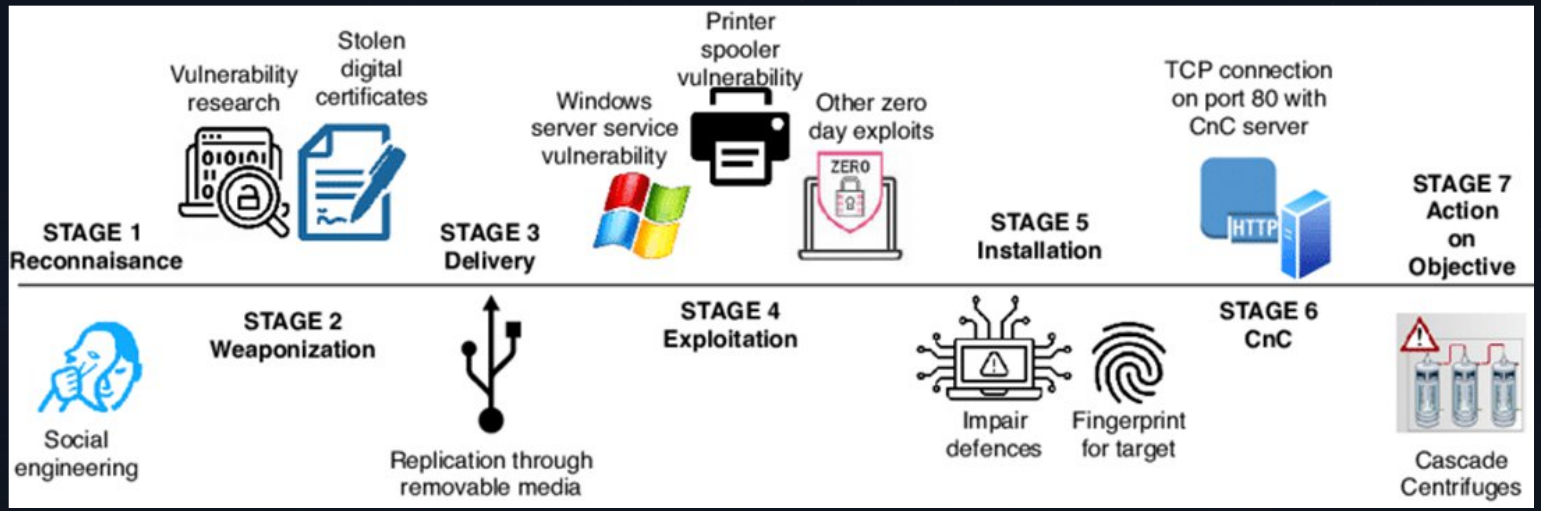
Часто застарілі технології та відсутність вбудованих функцій безпеки

Ці фактори вимагають особливо ефективного управління та нагляду за SCADA-системами.

3.1.3. Урок Stuxnet: Ізоляція не гарантує безпеку

Інцидент зі Stuxnet, який був добре вивченим і задокументованим руткітом, використаним на SCADA-системі, демонструє успішну атаку на об'єкт, який був фізично ізольований від зовнішніх мереж.

Це підкреслює, що навіть "ізольовані" системи не застраховані від загроз, якщо фізична безпека скомпрометована. Stuxnet показав, як зловмисники можуть використовувати фізичний доступ для впровадження шкідливого програмного забезпечення навіть у повністю відокремлені від мережі системи.



3.1.4. Природа загроз для IACS

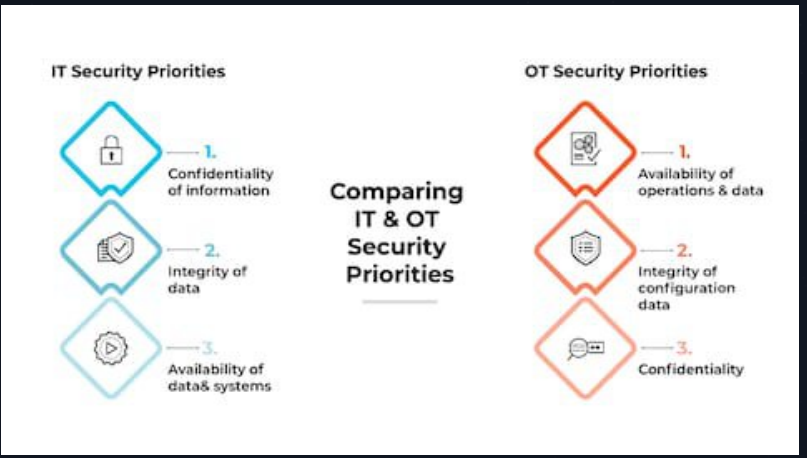
Злочинні атаки

- Умисні кібератаки з злочинним мотивом
- Цілеспрямовані атаки на критичну інфраструктуру
- Промислове шпигунство

Ненавмисні загрози

- Незначна поведінка працівника
- Помилки при форматуванні систем
- Втрата важливих даних через недбалість

Безпека в системах промислової автоматизації та керування (IACS) розглядається як захист промислових підприємств від несанкціонованих фізичних та цифрових атак.



3.1.5. Пріоритети безпеки: ICS/OT vs IT

Доступність

Першочерговий пріоритет у системах IACS

Цілісність

Другий за важливістю пріоритет

Конфіденційність

Третій пріоритет у промислових системах

На відміну від традиційних IT-систем, де пріоритетом є конфіденційність, цілісність та доступність даних (CIA-тріада), у системах IACS доступність є першочерговим пріоритетом.

3.1.6. Кінетичний вплив порушень ICS/OT

Травми персоналу

Порушення в роботі промислових систем може призвести до серйозних травм або загибелі працівників

Екологічна шкода

Аварії можуть спричинити значну шкоду навколишньому середовищу та екосистемам

Зупинка виробництва

Простої виробництва призводять до значних економічних втрат та порушення ланцюгів поставок

3.2. Фундаментальна роль фізичної безпеки

Фізична безпека є основою для забезпечення безперервності операцій та захисту людей та навколишнього середовища.

Незважаючи на прогрес у кібербезпеці, фізичний доступ залишається одним із найефективніших векторів атаки. Рекомендується розглядати фізичну безпеку як невід'ємну частину загальної стратегії кібербезпеки, приділяючи їй таку ж, якщо не більшу, увагу, як і цифровим загрозам.

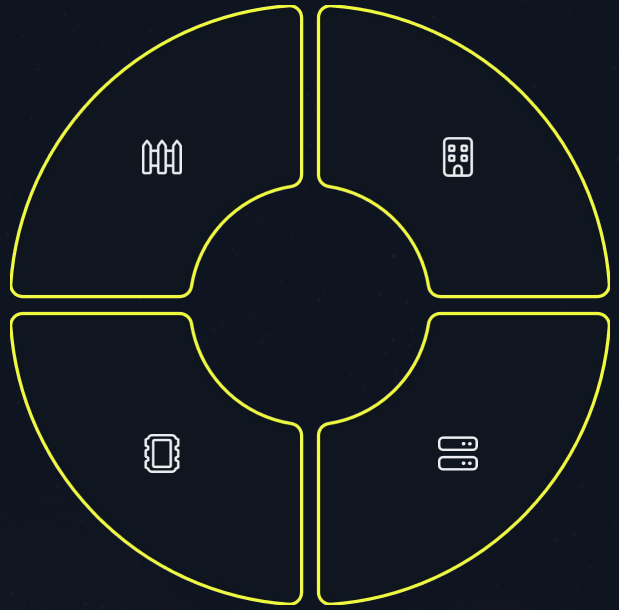
3.2.1. Багаторівневі фізичні заходи безпеки

Периметр

Зовнішні огорожі та контроль доступу

Будівля

Контроль доступу до приміщень



Пристрої

Фізичний захист окремого обладнання

Критичні зони

Захист серверних та операційних кімнат

Для захисту об'єктів ICS важливо впроваджувати багаторівневі фізичні заходи безпеки. Це допомагає створити "захист в глибину" (Defense-in-Depth) на фізичному рівні.

3.2.2. Огорожі та ворота: Перший рубіж оборони

Базові, але ефективні заходи

Використання огорож та воріт для контролю доступу транспортних засобів та персоналу є базовим, але ефективним заходом захисту промислових об'єктів.

- Контроль доступу транспортних засобів
- Обмеження пішохідного доступу
- Візуальне стримування потенційних порушників
- Створення контрольованих точок входу

3.2.3. Високозахищені ключові системи

Замки на дверях

Контроль доступу до критичних приміщень та зон обслуговування обладнання

Замки на шафах

Захист електричних панелей, серверних шаф та розподільних щитів

Замки на пристроях

Фізичний захист окремих компонентів системи та термінальних пристроїв

Високозахищені ключові/замкові системи є важливими для обмеження фізичного доступу до критичних зон та пристроїв.

3.2.4. Електронні системи контролю доступу

Переваги електронних систем

- Гнучке управління доступом
- Реєстрація всіх подій доступу
- Можливість швидкого відкликання доступу
- Інтеграція з іншими системами безпеки
- Часові обмеження доступу

Електронні системи доповнюють механічні замки, надаючи більш гнучке управління доступом та можливість реєстрації подій.

3.2.5. Контроль доступу до PLC

На програмованих логічних контролерах (PLC) фізичний ключ-перемикач контролює режими роботи (наприклад, "програма" або "виконання").

01

Режим програмування

Дозволяє модифікацію логіки контролера

02

Режим виконання

Блокує зміни та забезпечує стабільну роботу

03

Контроль оновлень

Регулює можливість віддаленого оновлення прошивки

3.2.6. Захист кабелів та обладнання

Прокладання кабелів

Кабелі слід прокладати таким чином, щоб мінімізувати доступ до них, обмежуючи його лише авторизованому персоналу.

Встановлення обладнання

Обладнання необхідно встановлювати в закритих шафах з належною вентиляцією та фільтрацією повітря.

Вибір кабелів

Неекранований кабель крученої пари не підходить для промислового середовища через чутливість до електромагнітних полів, радіохвиль, екстремальних температур, вологи, пилу та вібрації.

3.2.7. Рекомендовані типи кабелів

Волоконно-оптичні кабелі

Стійкі до електромагнітних перешкод та екстремальних умов промислового середовища

Коаксіальні кабелі

Забезпечують надійну передачу сигналів у важких промислових умовах

Для контрольних мереж краще використовувати волоконно-оптичні або коаксіальні кабелі, які стійкі до промислових умов експлуатації.

3.2.8. Документація та інвентаризація

1 **Маркування кабелів**

Кабелі та роз'єми повинні бути марковані та кольорово кодовані, щоб чітко розрізняти мережі ICS та IT

2 **Документування доступу**

Всі авторизовані телефонні лінії та орендовані лінії для послідовного зв'язку повинні бути точно задокументовані

3 **Заходи захисту**

Список має включати заходи захисту: зворотний виклик, шифруючі модеми, VPN, ручне підключення модему

3.3. Інтеграція фізичних та кібербезпекових заходів

3.3.1. Комплексна політика фізичної безпеки

Ефективні заходи фізичного контролю доступу є багатошаровими і включають як прості механічні бар'єри, так і складні електронні системи.

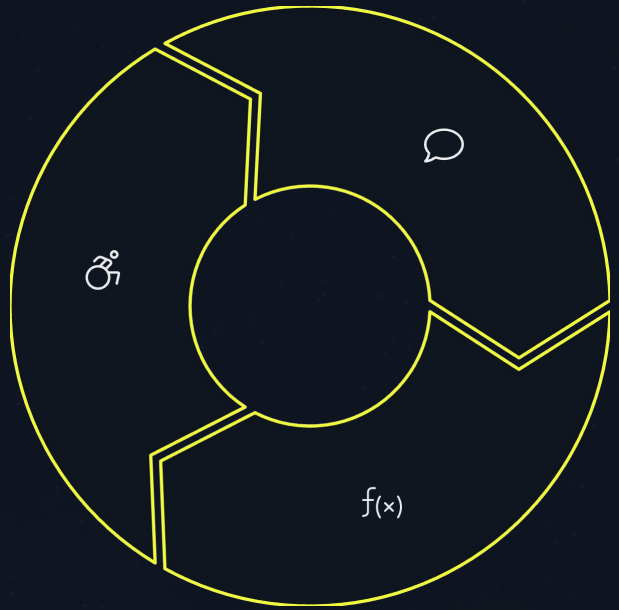
Рекомендація: Розробляти та впроваджувати комплексну політику фізичної безпеки, що охоплює всі активи ICS/SCADA, від зовнішнього периметра до окремих пристроїв.

Важливо також регулярно переглядати та оновлювати ці заходи, а також забезпечувати сувору документацію всіх точок доступу та захисних механізмів.

3.3.2. Взаємне посилення безпеки

Фізична безпека

Контроль доступу та захист периметра



Кібербезпека

Захист мережевих з'єднань та даних

Функціональна безпека

Забезпечення безпечної роботи процесів

Фізичні та кіберзаходи безпеки повинні бути інтегровані, оскільки вони взаємно посилюють одна одну. Забезпечення промислової безпеки включає в себе як інформаційну безпеку/кібербезпеку, так і функціональну безпеку.

3.3.3. Співпраця між фахівцями

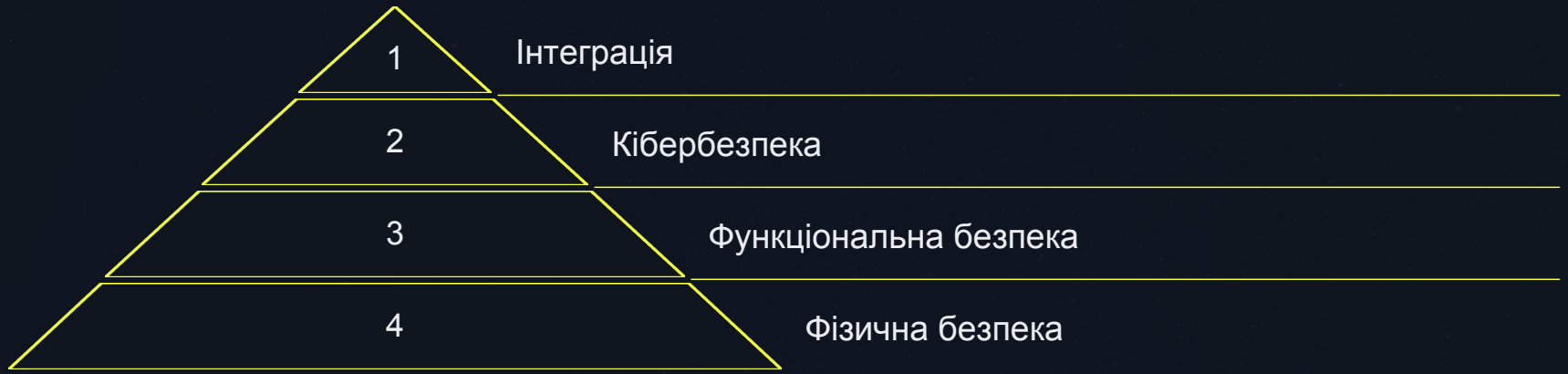
Виклики інтеграції

- Прогалини у культурі між IT та OT
- Різниця у знаннях та досвіді
- Відмінності у пріоритетах безпеки
- Різні підходи до управління ризиками

Фахівці з кібербезпеки та функціональної безпеки повинні співпрацювати для забезпечення загальної безпеки.

Це передбачає подолання прогалин у культурі, знаннях та досвіді між персоналом IT та OT.

3.3.4. Єдиний фреймворк безпеки



Питання поєднання вимог кібербезпеки з вимогами функціональної безпеки є критичним, оскільки системи промислової автоматизації керують фізичними, потенційно небезпечними об'єктами.

Існує потреба в міждисциплінарній інтеграції зусиль та знань, оскільки загрози походять не тільки від зловмисників, але й від некомпетентного персоналу, відмов обладнання та впливів навколишнього середовища.

3.3.5. Середовище безпеки за IEC TR 63069:2019

> Середовище безпеки – це загальний набір контрзаходів, необхідних для забезпечення ефективно захищеного середовища для виконання функцій функціональної безпеки, і воно не обмежується лише захистом цих функцій.

Технічний звіт IEC TR 63069:2019 запроваджує ідею "середовища безпеки" (security environment) для узгодження співпраці між доменами функціональної безпеки та кібербезпеки.

3.3.6. Керівні принципи інтеграції

1

Захист функціональної безпеки

Заходи безпеки (security) повинні ефективно запобігати або захищати від несприятливих наслідків загроз системам функціональної безпеки

2

Захист функціоналу безпеки

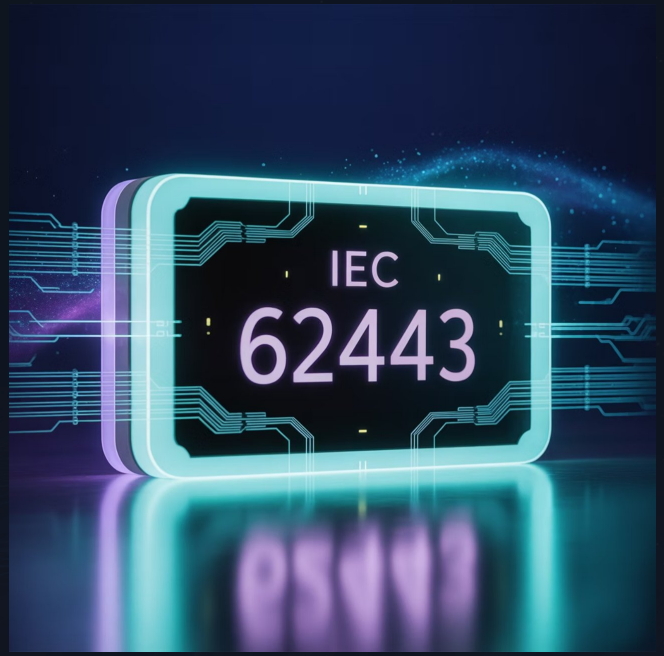
Заходи функціональної безпеки (safety) не повинні негативно впливати на ефективність впровадження безпеки (security)

3

Сумісність впроваджень

Реалізація функціоналу функціональної безпеки та реалізація функцій безпеки не повинні мати несприятливих суперечностей

3.3.7. Застосування стандартів ISA 99 / IEC 62443



Подолання розриву

Стандарти ISA 99 / IEC 62443 розроблені для подолання розриву між операційними та інформаційними технологіями, а також між функціональною безпекою процесів та кібербезпекою.

Гнучка структура

Вони забезпечують гнучку структуру для вирішення вразливостей і застосування засобів пом'якшення систематичним способом.

3.3.8. Рекомендації щодо інтеграції

Єдиний фреймворк

Розробляти єдиний фреймворк безпеки, який враховує взаємодію всіх аспектів – від фізичного доступу до мережевих протоколів

Керування стандартами

Підхід, керований стандартами на кшталт IEC 62443 та IEC 61508, забезпечить відсутність нових вразливостей

Навчання персоналу

Постійно навчати персонал та забезпечувати взаємодію між фахівцями IT, OT та фізичної безпеки

3.4. Висновки: Комплексний підхід до безпеки

Ефективна безпека в ICS/SCADA досягається лише через інтеграцію фізичних та кібербезпекових заходів.

Фізична безпека як основа

Забезпечення фізичного захисту є першим кроком до досягнення доступності, цілісності та безпеки промислових процесів

Інтегрований підхід

Рішення щодо безпеки не повинні створювати нових вразливостей в інших областях і впливати на критичну доступність систем

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!