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

Лекція 4: **Реагування на інциденти, відновлення після збоїв та судова експертиза.**

Мета лекції

Сформувати практичну готовність до реагування на інциденти, відновлення та цифрової криміналістики в ICS/SCADA з пріоритетом безпеки людей і безперервності процесу

Основні завдання

Вибудувати OT-орієнтований процес Incident Response
Підготовка, ідентифікація, стримування, викорінення, відновлення, уроки.

Забезпечити стійкість через DR/BC
Планування, сценарні тренування (tabletop, functional, full-scale), робота в режимі operate-through.

Запровадити надійну стратегію резервного копіювання й відновлення
Склад, періодичність, офлайн/георезерв, регулярні тести відновлення.

Розвинути цифрову криміналістику для OT
Збір і збереження доказів без зупинки процесу, робота з OT-протоколами та журналами.

Синхронізувати IT та OT-команди
Чіткі ролі, зміни за процедурою, актуальна документація, інтеграція з SIEM/IDS.

Підвищити готовність персоналу
Навчання, тренування, культура кібер-обізнаності, врахування локальних викликів і стандартів IEC 62443.

4.1. Планування та процедури реагування на інциденти для ICS/SCADA

4.1.1. Життєвий цикл реагування на інциденти

01

Підготовка

Розробка політик, процедур, створення команди реагування на інциденти (CSIRT), встановлення інструментів та технологій для ефективного реагування.

02

Ідентифікація

Виявлення інциденту через SIEM та інші системи захисту. Повідомлення про несприятливі події повинні оцінюватися та оброблятися персоналом.

03

Стримування

Обмеження впливу інциденту для запобігання подальшому поширенню загрози по системі та мережі.

04

Викорінення

Видалення причини інциденту та всіх скомпрометованих компонентів з системи для повного усунення загрози.

05

Відновлення

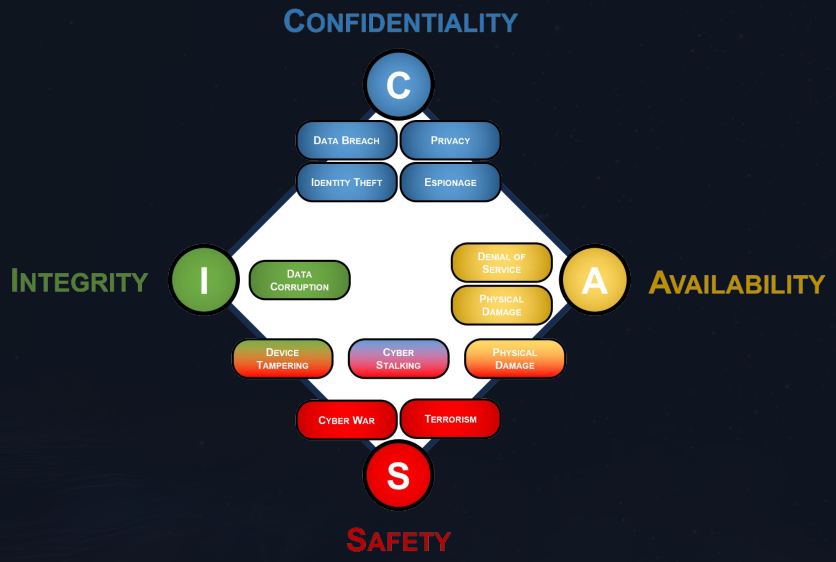
Повернення скомпрометованих систем до нормальної роботи з дотриманням всіх вимог безпеки.

06

Отримані уроки

Аналіз інциденту, виявлення слабких місць та внесення змін для запобігання подібним інцидентам у майбутньому.

4.1.2. Унікальні пріоритети в ICS/SCADA системах



На відміну від традиційних IT-систем, де пріоритетами є конфіденційність, цілісність та доступність даних (CIA-тріада), в ICS/OT середовищах пріоритети кардинально відрізняються:

Фізична безпека (Safe)
Безпека людей та навколишнього середовища є першочерговою. Порушення безпеки в OT може призвести до травм або зупинки виробництва.

Доступність (Availability)
Безперервна робота систем є критичною. Зупинка може спричинити значні економічні збитки та збої в критичній інфраструктурі.

Цілісність (Integrity)
Гарантія того, що дані не були змінені несанкціонованим чином та відображають реальний стан процесів.

Конфіденційність (Confidentiality)
Займає менш високий пріоритет, оскільки дані часто знаходяться в необробленому вигляді.

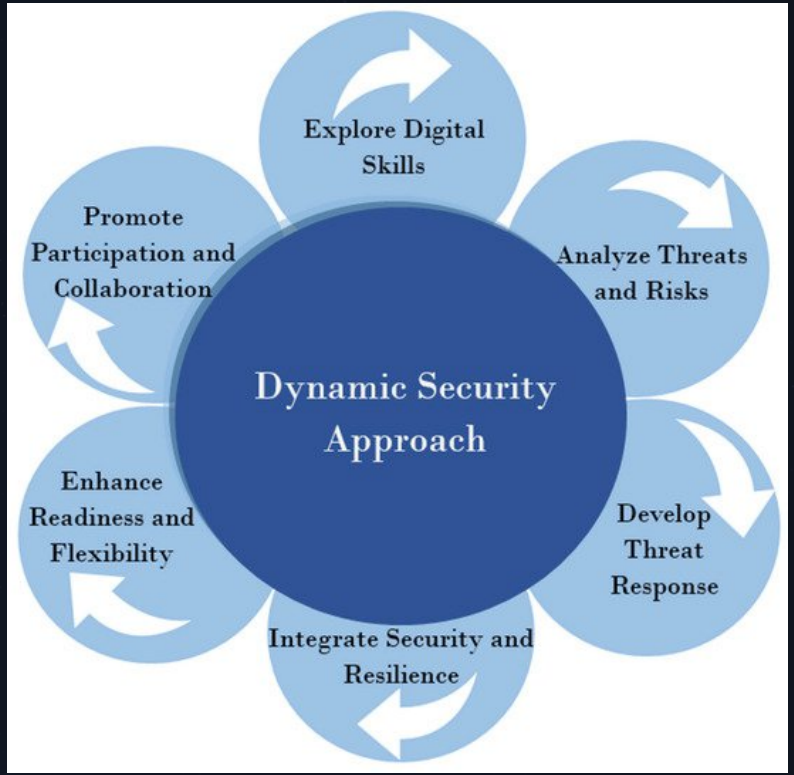
4.1.3. Рекомендації для планування реагування на інциденти

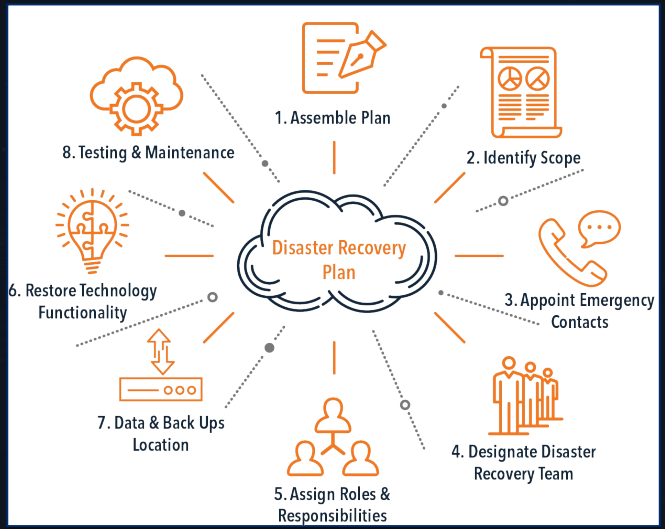
Ключові принципи

- Розробка спеціалізованих планів, які враховують унікальні пріоритети OT та потенційні фізичні наслідки
- Забезпечення тісної співпраці між IT- та OT-командами реагування на інциденти
- Проведення регулярних навчань та симуляцій інцидентів
- Ретельна документація всіх процедур та їх постійне оновлення

Плани реагування на інциденти для ICS/SCADA повинні бути послідовними та інтегрованими з існуючим досвідом, програмами та практиками IT-безпеки, але адаптовані до конкретних вимог та характеристик ICS-технологій.

4.2. Відновлення після збоїв та безперервність бізнесу для систем SCADA





4.2.1. Відновлення після збоїв та безперервність бізнесу

Планування відновлення після збоїв (Disaster Recovery, DR) та забезпечення безперервності бізнесу (Business Continuity, BC) є критично важливим для систем SCADA. Управління кібербезпекою — це постійна діяльність, яка вимагає безперервного вдосконалення.

1

Disaster Recovery (DR)

Зосереджується на відновленні IT-систем та даних після катастрофічної події. Включає відновлення контролерів, серверів, HMI та комунікаційних мереж.

2

Business Continuity (BC)

Забезпечує продовження критично важливих бізнес-функцій навіть під час збоїв. Підтримка технологічного процесу через ручне управління або автономні системи.

4.2.2. Типи тестів для DR/BC у SCADA системах

Орієнтаційні семінари

Менш активні заходи з низьким залученням агентств. Базовий рівень підготовки персоналу до можливих сценаріїв.

Тренування

Більш активні та залучені заходи з інтенсивними, повністю імітованими повідомленнями та практичними вправами.

Настільні навчання

Середній рівень активності з наративними сценаріями та менш інтенсивними повідомленнями для аналізу дій.

Функціональні тести

Високий рівень активності, спрямований на висвітлення конкретних функцій та процедур системи.

Повномасштабні тести

Найвищий пріоритет з інтенсивною передачею симульованих повідомлень у реальному часі та повним залученням всіх систем.

4.3. Стратегії резервного копіювання та відновлення

4.3.1. Стратегії резервного копіювання та відновлення

Регулярне резервне копіювання та перевірка процедур відновлення є необхідними для забезпечення стійкості системи ICS/SCADA. Ці заходи є частиною фази технічного обслуговування життєвого циклу кібербезпеки.

Визначення елементів

Політики повинні чітко вказувати, які дані та конфігурації потребують резервного копіювання, включаючи конфігураційні таблиці SCADA-системи.

Інтервал та кількість

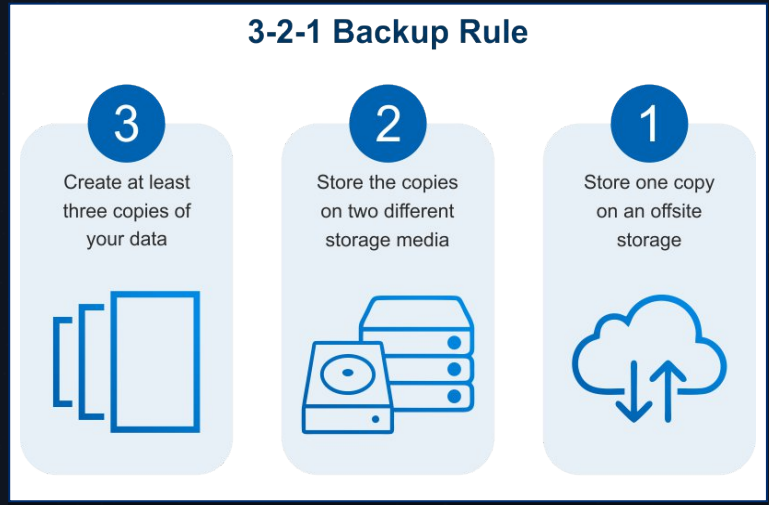
Визначення частоти резервного копіювання (щоденно, щотижнево) та кількості копій для зберігання.

Метод копіювання

Вказується, чи резервне копіювання є ручним чи автоматичним, з урахуванням специфіки промислового середовища.

Безпечне зберігання

Резервні копії повинні зберігатися в безпечному місці, бажано віддалено, щоб запобігти компрометації разом з основною системою.



4.3.2. Важливість тестування відновлення

Критичні аспекти

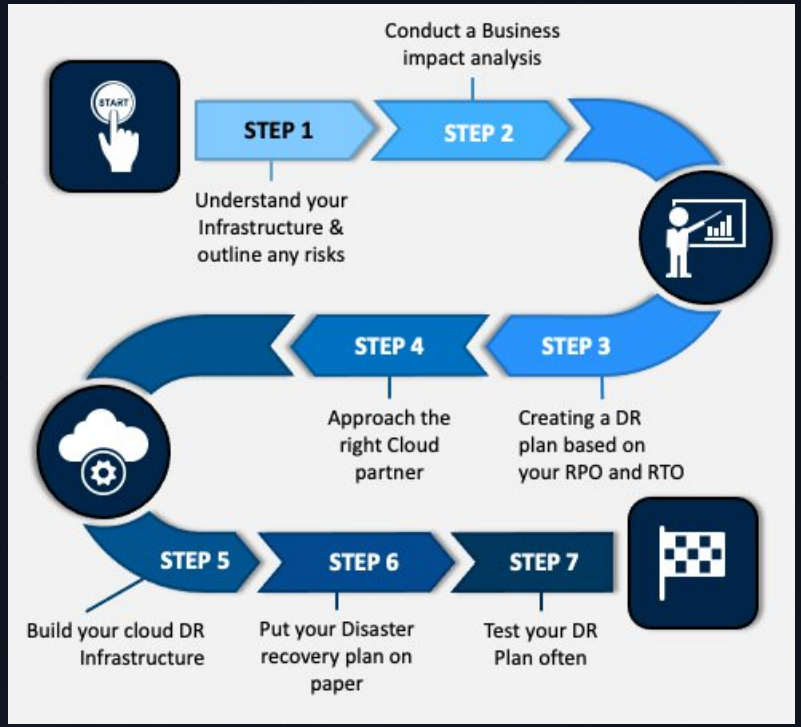
Регулярна перевірка як резервного копіювання файлів, так і відновлення функціональності є важливою для гарантування функціонування системи в разі інциденту безпеки.

> Реальний випадок: Власник SCADA-системи оновив обладнання, замінивши магнітні стрічкові накопичувачі на Blu-ray DVD, але виявив, що системна резервна копія все ще зберігалася на магнітних стрічкових картриджах під час настільного огляду процедури відновлення.

Це підкреслює критичну важливість актуальності та регулярного тестування систем резервного копіювання.

Ключові рекомендації

- Автоматизація процесів резервного
- Моніторинг успішності операцій
- Періодичні тести відновлення
- Актуалізація технологій зберігання



4.4 Цифрова криміналістика в середовищах SCADA

4.4.1. Цифрова криміналістика в середовищах SCADA

Цифрова криміналістика у середовищах SCADA — це спеціалізована дисципліна, яка включає збір, збереження, аналіз та представлення цифрових доказів з ICS/OT систем після інциденту безпеки. Це критично важливий етап для розуміння інциденту та запобігання подібним у майбутньому.

Пріоритет доступності

На відміну від IT-криміналістики, у OT-середовищі доступність системи є першочерговим пріоритетом, що ускладнює збір доказів.

Специфічні протоколи

ICS/SCADA використовують унікальні протоколи (Modbus, DNP3, S7) та спеціалізоване обладнання, що вимагає особливих знань.

Аналіз журналів

Аналіз журналів є ключовим для виявлення інцидентів та підтримки ситуаційної обізнаності в промислових системах.

4.4.2.Особливості криміналістики в промислових системах

1

Взаємозв'язок з фізичним світом

Атаки на ICS/SCADA системи часто мають фізичні прояви, що може бути джерелом додаткових доказів, але також ускладнює розслідування.

2

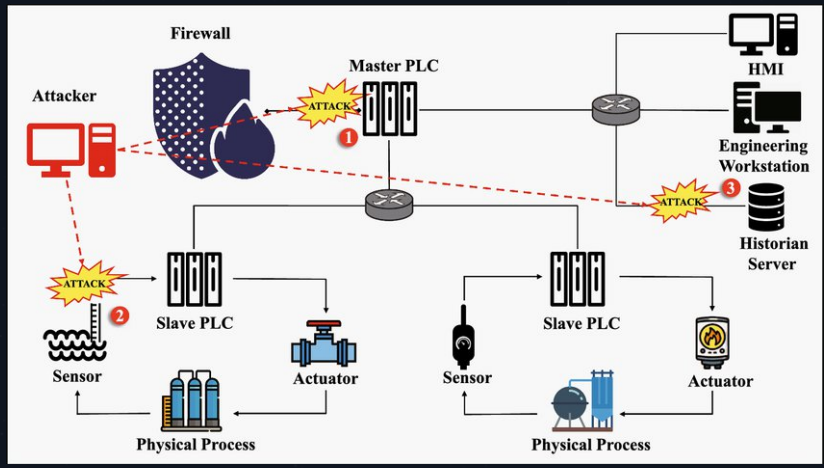
Приховування інформації

За оцінками, 80% компаній приховують навіть сам факт кібератак через іміджеві та фінансові ризики, що обмежує обмін знаннями.

3

"Сліпі зони"

У промислових мережах існують "сліпі зони" через віддалений контроль виробником обладнання, що ускладнює криміналістику.



4.4.3.Рекомендації для цифрової криміналістики

1 Спеціалізована підготовка

Інвестуйте в навчання персоналу для отримання спеціалізованих навичок у галузі цифрової криміналістики для ICS/OT.

2 Розробка процедур

Створіть чіткі процедури для збору та збереження цифрових доказів у виробничому середовищі.

3 Використання інструментів

Використовуйте спеціалізовані інструменти для збору та аналізу даних з ICS/OT систем.

4 Обмін інформацією

Беріть участь в інформаційних обмінах для отримання досвіду про TTPs зловмисників.

Цифрова криміналістика в ICS/OT є складною, але вкрай важливою для повного розуміння інцидентів та постійного вдосконалення безпеки промислових систем.

4.5. Навчання та обізнаність персоналу з реагування на інциденти

4.5.1. Людський фактор у кібербезпеці

Людський фактор є однією з головних причин кіберінцидентів. Міжнародна статистика показує, що більшість кіберінцидентів спричинена саме ним. Тому навчання та підвищення обізнаності персоналу є ключовим для мінімізації цього фактора.

80%

Інциденти через людський фактор

Більшість кіберінцидентів спричинена помилками або недбалістю персоналу

70%

Успішність навчання

Регулярне навчання знижує ризик інцидентів на 70% порівняно з необученим персоналом

90%

Швидкість реагування

Навчений персонал реагує на інциденти на 90% швидше за ненавчений

4.5.2. Критичність навчання персоналу

Зменшення людських помилок

Працівник може ненавмисно занести шкідливе програмне забезпечення або виконати дії, що призведуть до втрати важливих даних. Навчання допомагає мінімізувати такі ризики.

Культура кібер-обізнаності

Важливо встановити культуру кібер-обізнаності, де оператори розуміють взаємозв'язок між кібер- та фізичними системами.

Ефективне реагування

Навчений персонал швидше та ефективніше виявлятиме, стримуватиме та відновлюватиме системи після інцидентів. Персонал повинен мати глибокі знання застосунків моніторингу.

Імплементація стандартів

Відповідні програми навчання можуть бути використані для навчання персоналу впровадженню стандартів, таких як ISA 99 / IEC 62443.

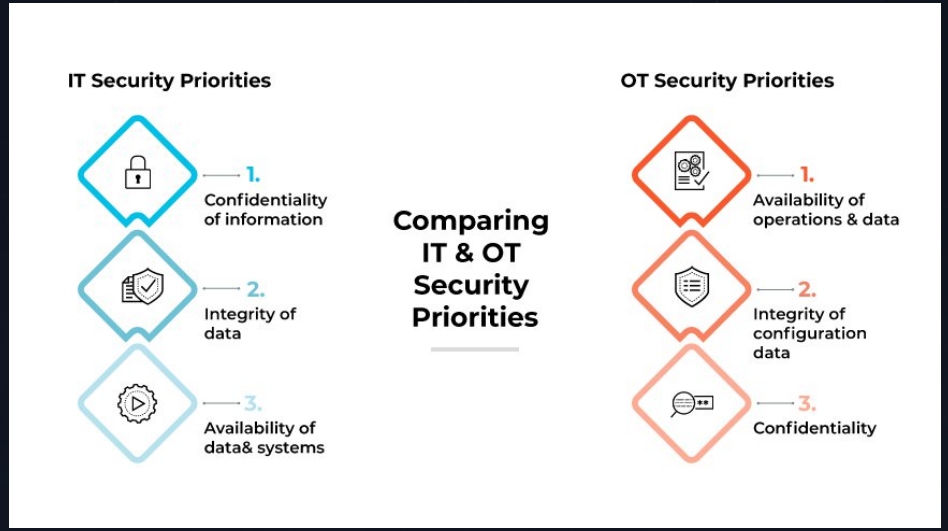
4.5.3. Відмінності між IT та OT персоналом

Проблемні аспекти

У більшості компаній все ще існують прогалини у культурі, знаннях та досвіді між представниками персоналу з інформаційних та операційних технологій.

- Необачність фахівців АСК ТП щодо безпеки власних мереж
- Рідкість відомих кіберзагроз у промисловій галузі
- Розподіл відповідальності між групами IT та OT
- Різні підходи до пріоритетів безпеки

Ефективна кібербезпека вимагає тісної співпраці між IT та OT командами, розуміння специфіки кожного домену та спільного підходу до управління ризиками.



4.5.4.Виклики впровадження кібербезпеки в Україні

Скептичне відношення
В Україні існує скептичне відношення до стандартів кібербезпеки з боку виробничників та інтеграторів промислових систем.

Брак фахівців
Відсутність фахівців, здатних підтримувати впровадження стандартів, є однією з найбільших проблем у галузі.

Необізнаність керівництва
Необізнаність керівництва та інтеграторів про можливості та необхідність кібербезпеки є значним викликом.

Відсутність спеціалізованих підрозділів
На критичних об'єктах часто немає відокремлених підрозділів кібербезпеки; функції розподілені між різними службами.

4.5.5.Шляхи вирішення проблем в Україні

1

Навчання спеціалістів

Учасники (замовники, провайдери, галузеві асоціації) можуть почати навчати своїх спеціалістів, в тому числі за кордоном, для отримання необхідних компетенцій.

2

Створення підрозділів

Створення відокремлених підрозділів з відповідними повноваженнями для постійного забезпечення кібербезпеки промислових систем.

3

Підготовка з IEC 62443

Важливим етапом є підготовка спеціалістів щодо розуміння серії IEC 62443 у контексті кібербезпеки промислових систем керування.

4.5.6. Міжнародні проекти модернізації навчання

Проект SEREIN

Міжнародний проект з модернізації навчальних курсів з кібербезпеки, який надає сучасні методики та матеріали для підготовки фахівців у галузі промислової кібербезпеки.

Проект ALIOT

Спеціалізований проект, присвячений кібербезпеці Інтернету Речей, який включає аспекти захисту промислових IoT-пристроїв та систем.

Така підготовка може базуватися на результатах цих міжнародних проектів та адаптуватися до специфічних потреб української промисловості та критичної інфраструктури.

4.5.7. Комплексні програми навчання персоналу

Розробіть та впровадьте регулярні програми навчання з кібербезпеки для всіх рівнів персоналу, враховуючи як IT-, так і OT-специфіку промислових систем.

4.5.8. Практичні тренування та симуляції

Симуляції інцидентів

Практичні симуляції кіберінцидентів для відпрацювання навичок реагування в контрольованому середовищі.

Використання інструментів

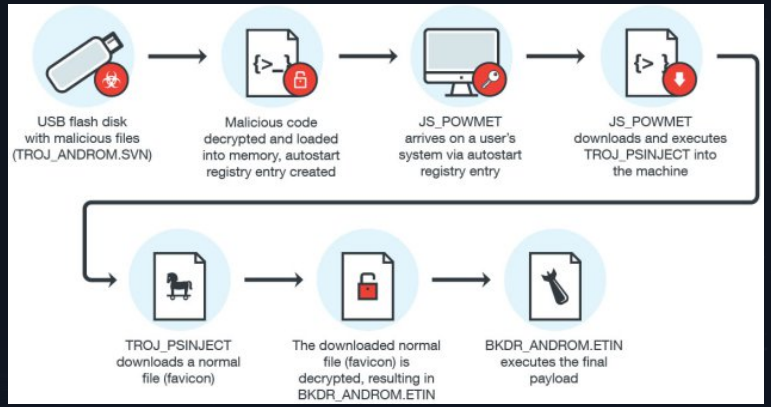
Навчання роботі з інструментами моніторингу, виявлення загроз та реагування на інциденти.

Аварійні процедури

Відпрацювання аварійних процедур та координації дій між різними службами під час кіберінцидентів.

Включіть у навчання практичні тренування для підвищення навичок та готовності до реальних загроз у промислових

4.5.9. Основи кібер-гігієни для промислового персоналу



Безпечне використання знімних носіїв

Правила роботи з USB-накопичувачами, CD/DVD дисками та іншими знімними носіями в промислових мережах.

Розпізнавання фішингових атак

Навички виявлення підозрілих електронних листів, посилань та вкладень, особливо в контексті промислових систем.

Створення надійних паролів

Принципи створення та управління паролями для доступу до критично важливих промислових систем.

Безпечна робота з мережею

Правила підключення до промислових мереж, використання Wi-Fi та віддаленого доступу.

4.5.10. Культура кібер-обізнаності

Ключові принципи

Сприяйте створенню культури кібер-обізнаності, де кібербезпека розглядається як спільна відповідальність всіх співробітників організації.

- Кібербезпека як частина щоденної роботи
- Відкрите обговорення загроз та інцидентів
- Заохочення повідомлень про підозрілу активність
- Регулярне оновлення знань про нові загрози
- Інтеграція безпеки в робочі процеси

Культура кібер-обізнаності перетворює кожного співробітника на активного учасника системи кібербезпеки організації.

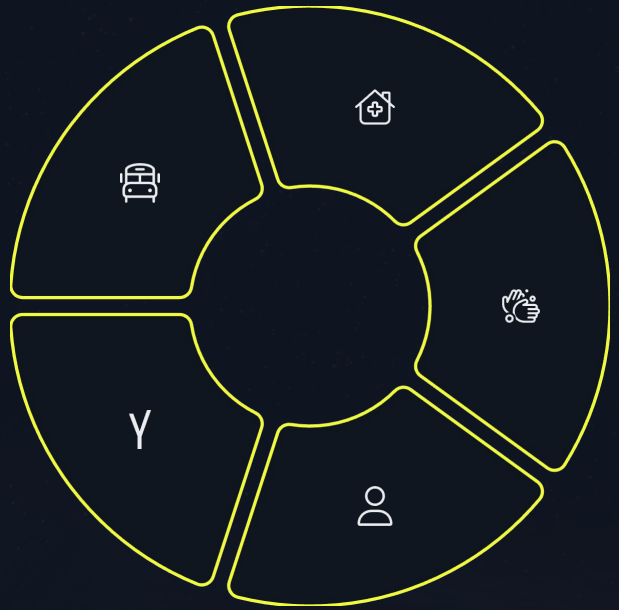
4.5.11. Рекомендації для ефективного навчання

Комплексні програми

Регулярні програми навчання для всіх рівнів персоналу

Міжнародний досвід

Використання проектів SEREIN та ALIOT



Практичні тренування

Симуляції інцидентів та використання інструментів

Кібер-гігієна

Основні правила безпечної роботи

Культура безпеки

Кібербезпека як спільна відповідальність

4.5.12. Інтеграція навчання з міжнародними стандартами

Підтримка міжнародних ініціатив та використання наявних навчальних матеріалів є ключовим для підвищення рівня кібербезпеки в Україні.

1. **Вивчення стандартів**

   Глибоке вивчення серії IEC 62443 та інших міжнародних стандартів кібербезпеки для промислових систем.

2. **Адаптація до місцевих умов**

   Адаптація міжнародного досвіду до специфічних потреб української промисловості та регуляторних вимог.

3. **Практичне впровадження**

   Поступове впровадження кращих практик з урахуванням технічних та організаційних можливостей підприємств.

4.6. Ключові висновки та

Планування реагування
Розробіть спеціалізовані плани реагування на інциденти, які враховують унікальні пріоритети OT та потенційні фізичні наслідки. Забезпечте тісну співпрацю між IT- та OT-командами.

Безперервність бізнесу
Створіть детальні плани DR/BC, які охоплюють усі компоненти SCADA та критичні бізнес-процеси. Проводьте регулярні та різноманітні тести планів.

Резервне копіювання
Розробіть чіткі політики резервного копіювання та проводьте періодичні тести відновлення. Забезпечте безпечне зберігання резервних копій.

Цифрова криміналістика
Інвестуйте в спеціалізовану підготовку персоналу та створіть процедури для збору цифрових доказів у виробничому середовищі.

Навчання персоналу
Розробіть комплексні програми навчання для всіх рівнів персоналу та створіть культуру кібер-обізнаності в організації.

4.7. Майбутнє кібербезпеки промислових систем

Управління кібербезпекою — це постійна діяльність, що вимагає безперервного вдосконалення для управління ризиками. Інвестиції в навчання та підвищення обізнаності персоналу є одними з найефективніших заходів кібербезпеки.

Стратегічні пріоритети

- Інтеграція IT та OT безпеки
- Розвиток спеціалізованих компетенцій
- Впровадження міжнародних стандартів
- Створення культури кібер-обізнаності
- Постійне вдосконалення процесів

Безпека

Через

Навчання

Ефективна кібербезпека промислових систем досягається через постійне навчання, адаптацію до нових загроз та створення культури безпеки на всіх рівнях організації.

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!