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

Лекція 2: Захист меж та контроль доступу

Мета лекції

Сформувати розуміння принципів захисту меж та контролю доступу в ICS/SCADA.

Роль міжмережевих екранів

Розкрити їх значення та правильне розміщення для захисту мереж.

Правила фільтрації та конфігурація

Вивчити створення безпечних правил фільтрації та налаштування систем.

Робота IDS/IPS

Ознайомитися з принципами функціонування та інтеграцією в моніторинг.

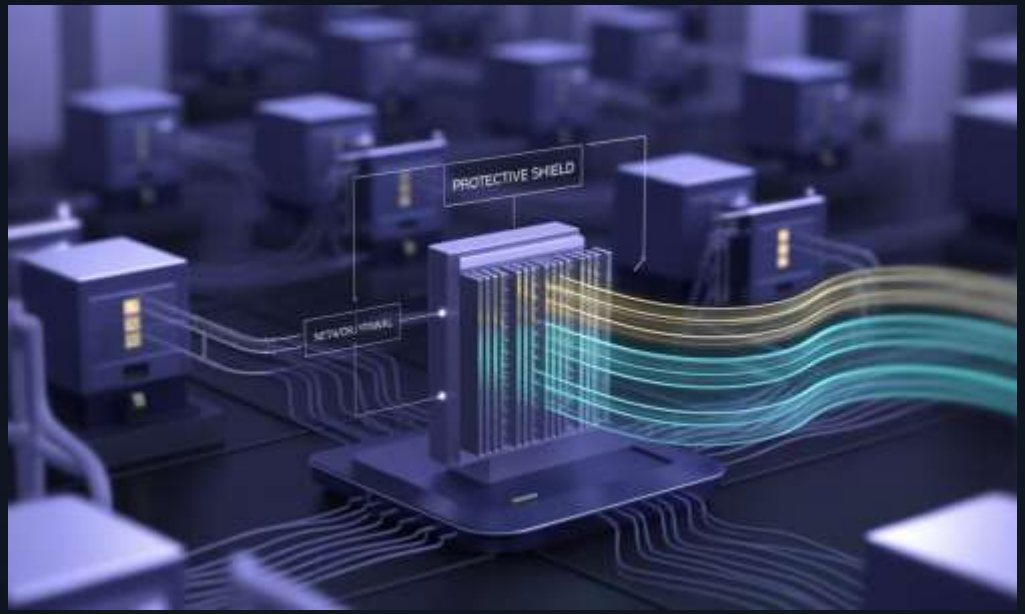
Механізми AAA

Засвоїти процеси автентифікації, авторизації та контролю доступу.

Принцип найменших привілеїв

Зрозуміти важливість мінімальних прав доступу та поділу обов'язків.

2.1. Впровадження та правила міжмережевих екранів

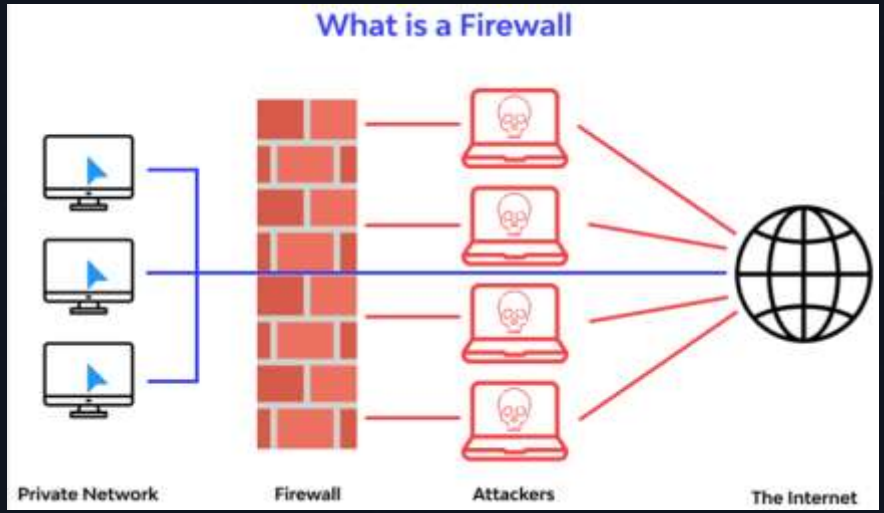


2.1.1. Роль міжмережевих екранів у промислових системах

Основне призначення

Міжмережеві екрани є основними компонентами безпеки, призначеними для захисту мережевих меж та контролю мережевого трафіку. Їхня функція полягає у фільтрації вхідних та вихідних пакетів на основі попередньо встановлених правил безпеки.

Це дозволяє створювати захищений периметр та реалізовувати сегментацію мережі, відокремлюючи різні мережеві сегменти, такі як корпоративна мережа від мережі керування.



2.1.2. Стратегічне розміщення міжмережевих екранів

Корпоративна мережа

Бізнес-домен з офісними системами та загальними IT-ресурсами

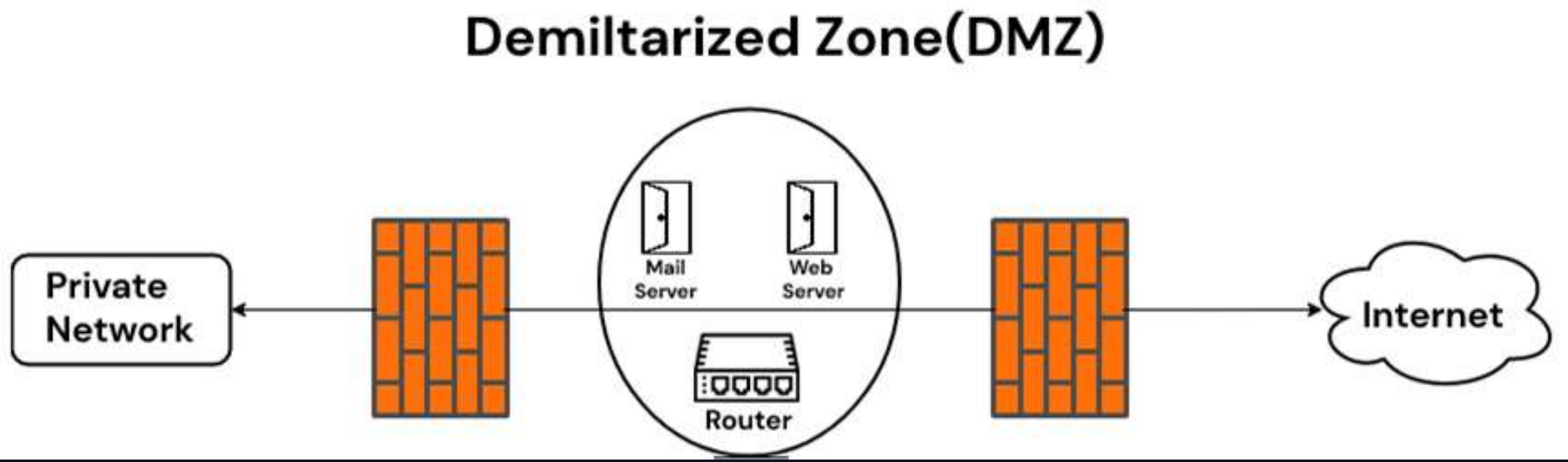
Міжмережевий екран

Контролює обмін операційними даними між доменами

OT-мережа

ICS-домен з промисловими системами контролю

У контексті промислових систем контролю (ICS) міжмережеві екрани зазвичай розміщуються між корпоративною мережею та мережею керування (OT-мережею). Це стратегічне розташування допомагає контролювати обмін операційними даними між ICS-доменом та бізнес-доменом.



2.1.3. Демілітаризована зона (DMZ)

Міжмережеві екрани також є невід'ємною частиною концепції демілітаризованої зони (DMZ), яка служить буфером для безпечної сегментації зовнішньої мережі від внутрішньої мережі IACS.

DMZ створює додатковий рівень захисту, дозволяючи контрольований доступ до певних ресурсів без прямого з'єднання із внутрішньою мережею.

2.1.4. Виклики та ризики міжмережевих екранів

Неправильне налаштування

Може призвести до несанкціонованого доступу або проникнення шкідливого програмного забезпечення до ICS-домену

Підтримка протоколів

Не всі міжмережеві екрани підтримують ICS-специфічні протоколи, що створює додаткові виклики

Управління змінами

Будь-які зміни в мережі можуть вимагати оновлення документації та правил міжмережевих екранів

2.1.5. Правила конфігурації міжмережевих екранів

Блокування непотрібних портів

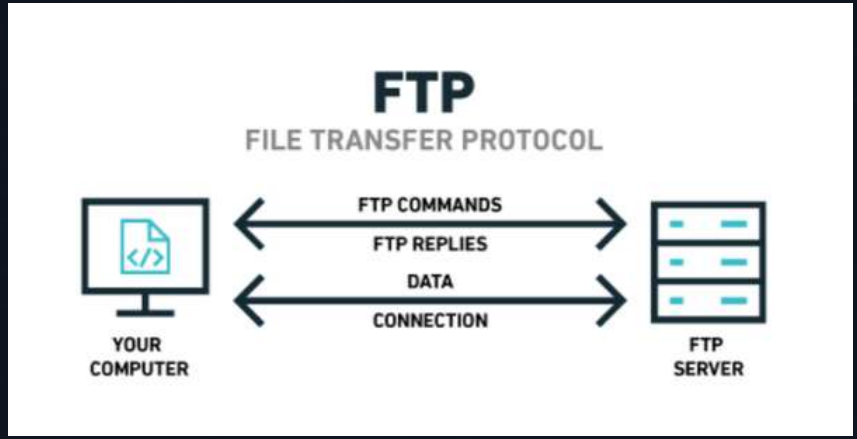
Наприклад, закриття порту 21 (FTP) може запобігти перехопленню незашифрованих даних та облікових даних, а також експлуатації вразливостей програмного забезпечення.

Документування

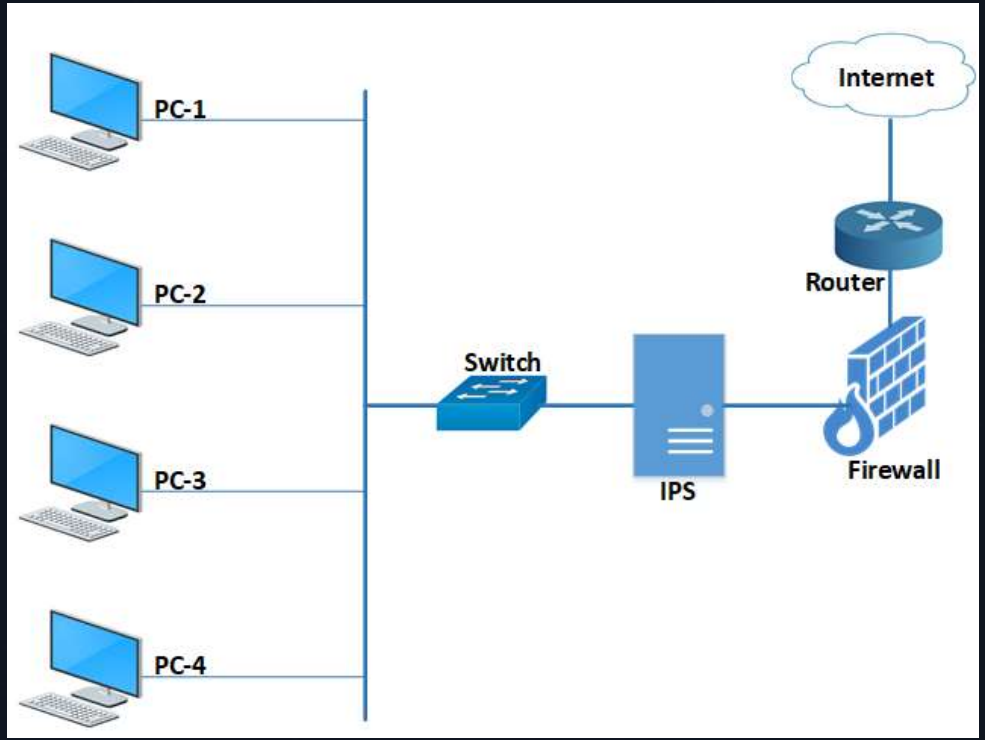
Важливо документувати всі фактичні комунікаційні з'єднання та захисні заходи, що застосовуються до точок доступу.

Оновлення профілів

Для міжмережевих екранів з функціями антивірусного захисту необхідне регулярне оновлення профілів вірусів.



2.2. Системи запобігання вторгненням (IPS)



2.2.1. Системи виявлення та запобігання вторгненням

IDS - Виявлення

Системи виявлення вторгнень в основному виявляють вторгнення як авторизованих, так і несанкціонованих користувачів

IPS - Запобігання

Системи запобігання вторгненням активно блокують виявлені атаки, доповнюючи функціонал міжмережевих екранів

Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) є важливими інструментами для забезпечення безпеки мереж ICS/OT.

2.2.2. Типи систем виявлення вторгнень

NIDS

Мережеві системи виявлення вторгнень моніторять мережевий трафік

HIDS

Хостові системи виявлення вторгнень моніторять окремі пристрої

Виявлення аномалій

Ідентифікація відхилень від нормальної поведінки

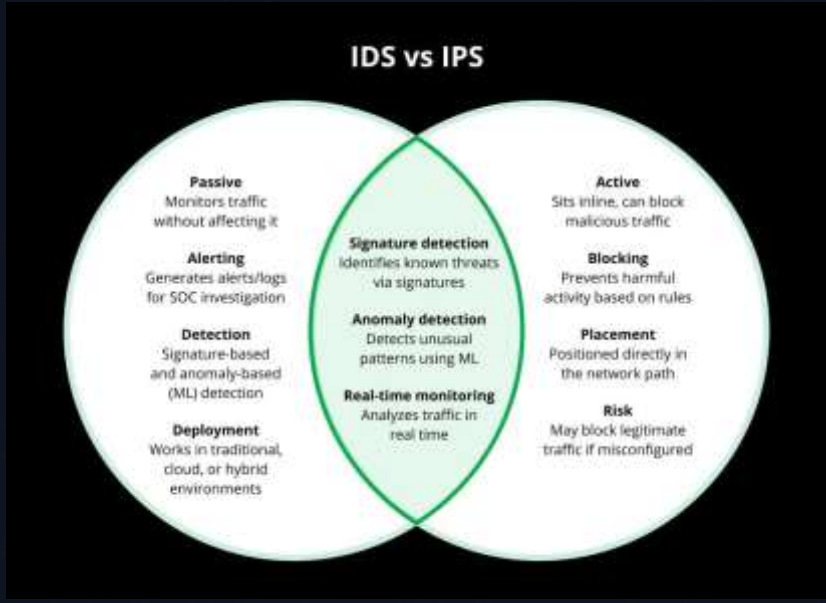
Сигнатурне виявлення

Порівняння з відомими шаблонами атак

2.2.3. Критичність правильного розміщення IDS/IPS

Засоби та системи захисту, включаючи IDS/IPS, можуть бути додані на етапі впровадження життєвого циклу кібербезпеки. Наприклад, в архітектурі, де використовується VPN, неправильне розміщення NIDS-сенсора може призвести до пропуску трафіку, що проходить через VPN-тунель.

Спеціалізовані засоби виявлення/запобігання кіберзагрозам мереж автоматизованих систем керування є важливим інструментом, оскільки цільова атака цілком може пройти міжмережеві екрани та досягти критичного об'єкта в нижніх сегментах промислової мережі.



2.2.4. Управління та моніторинг IDS/IPS

01

Постійний моніторинг

Відстеження технологій для виявлення шкідливої активності

02

Оцінка повідомлень

Аналіз сповіщень про несприятливі події персоналом

03

Обробка інцидентів

Використання процесу оброблення інцидентів для реагування

Ефективність IDS/IPS значною мірою залежить від знань персоналу, який їх налаштовує та моніторить. Працівники повинні мати глибокі знання додатків, розуміти хибні спрацювання систем захисту та вміти конфігурувати засоби для оптимізації їх точності.

2.2.5. Управління патчами для IPS

Управління патчами також є критично важливим для IPS, оскільки патчі використовуються для оновлення сигнатур шкідливих програм та усунення вразливостей.

Регулярне оновлення сигнатур та програмного забезпечення IPS/IDS, а також інтеграція їхніх сповіщень із загальною системою управління подіями безпеки (SIEM), посилить загальний захист.

2.3. Аутентифікація, авторизація та контроль доступу (AAA)

2.3.1. Концепція AAA: Аутентифікація, Авторизація, Контроль доступу

Authentication	Authorization	Access Control
Процес перевірки ідентичності користувача або системи. У системах IACS аутентифікація має високе значення	Процес визначення, які дії дозволено виконувати перевіреному користувачеві або системі	Механізми, які застосовують авторизаційні рішення, обмежуючи доступ до ресурсів

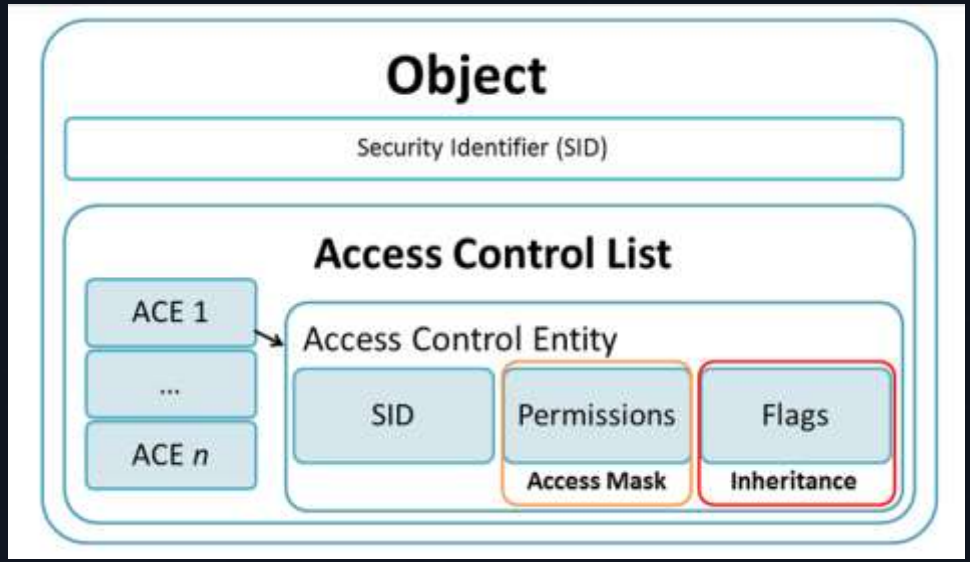
2.3.2. Мережевий контроль доступу

Жорсткий контроль точок доступу

Підтримка жорсткого контролю над точками доступу до ICS є необхідною, включаючи використання сильної автентифікації.

Списки контролю доступу (ACL)

Контроль доступу може бути реалізований на рівні даних за допомогою списків контролю доступу (ACL).



2.3.3. IP-комунікації та IPsec

Для IP-комунікацій, особливо в внутрішніх мережах, можуть використовуватися IPsec (Internet Protocol Security) для аутентифікації та шифрування пакетів.

IPsec забезпечує цілісність, конфіденційність та автентифікацію даних на мережевому рівні, що є критично важливим для захисту промислових комунікацій.

2.3.4. Специфічні промислові протоколи

1

ICCP протокол

Inter-Control Center Protocol в електроенергетиці підтримує базовий рівень аутентифікації (ACSE), хоча він є опціональним

2

Загальні механізми безпеки

Для забезпечення безпеки ICCP-з'єднань часто використовуються VPN та шифрування каналів

3

Modbus протокол

Є неавтентифікованим, що робить його вразливим до несанкціонованого читання/запису

2.3.5. Багатофакторна автентифікація (MFA)

Щось, що ви знаєте

Паролі, PIN-коди, секретні питання

Щось, що ви маєте

Смартфони, токени, смарт-карти

Щось, чим ви є

Біометричні дані: відбитки пальців, сітківка ока

Як загальний принцип кібербезпеки, багатофакторна автентифікація вимагає надання двох або більше доказів ідентифікації для отримання доступу.

2.3.6. Фізичні механізми контролю доступу

На програмованих логічних контролерах (PLC) фізичний ключ-перемикач контролює режими роботи (наприклад, "програма" або "виконання"), що є формою контролю доступу до функціоналу пристрою.

Це допомагає контролювати можливість віддаленого оновлення прошивки та програмування, забезпечуючи додатковий рівень фізичної безпеки.

2.3.7. Управління користувачами в SCADA-системах

Утиліта управління обліковими записами

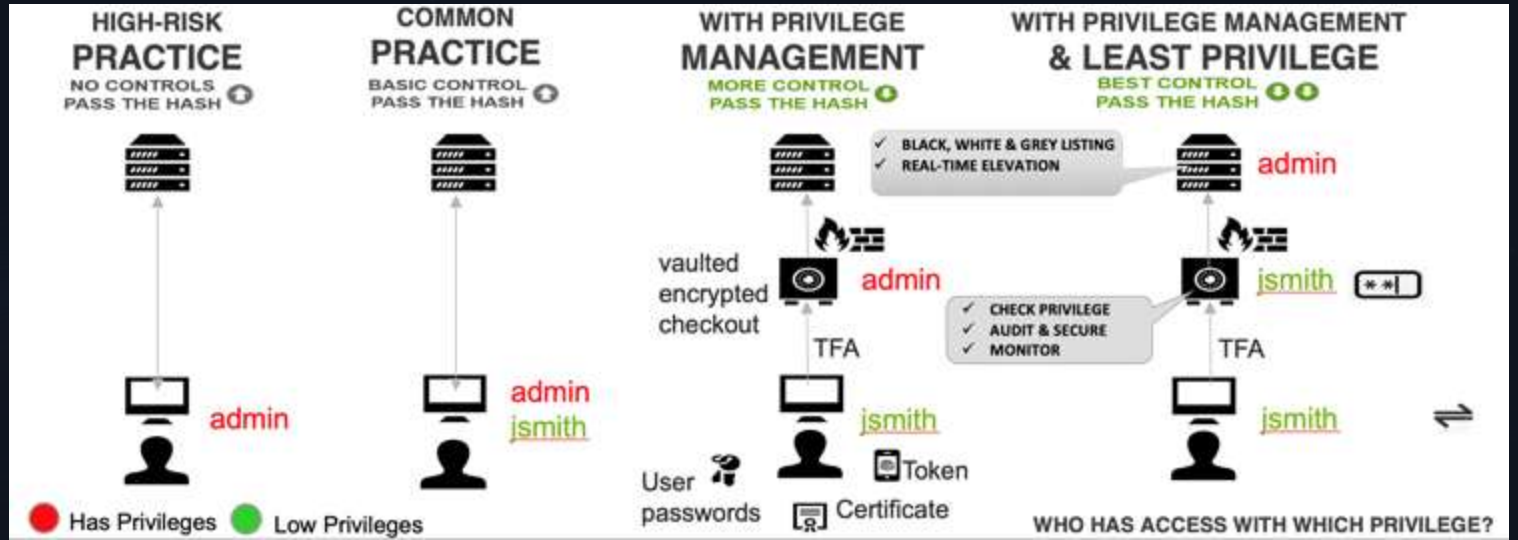
В SCADA-системах існує утиліта управління обліковими записами користувачів, яка дозволяє адміністраторам контролювати доступ та привілеї.

Унікальні облікові дані

Важливість використання унікальних облікових даних для IT та OT підкреслюється для забезпечення належної сегментації та контролю.

2.4. Принцип найменших привілеїв та поділ обов'язків

Принцип найменших привілеїв передбачає, що кожен користувач, програма або процес повинен мати лише мінімальний набір прав доступу, необхідний для виконання своїх законних функцій, і не більше того.



2.4.1. Реалізація принципу найменших привілеїв

1 Контроль доступу

Забезпечення жорсткого контролю над точками доступу до ICS та діагностичними дисплеями, а також над можливістю маніпулювання налаштуваннями

2 Обмеження програм та служб

Видалення або відключення всіх файлів та програм, які не є критично необхідними для функціонування промислової системи контролю

3 Управління документацією

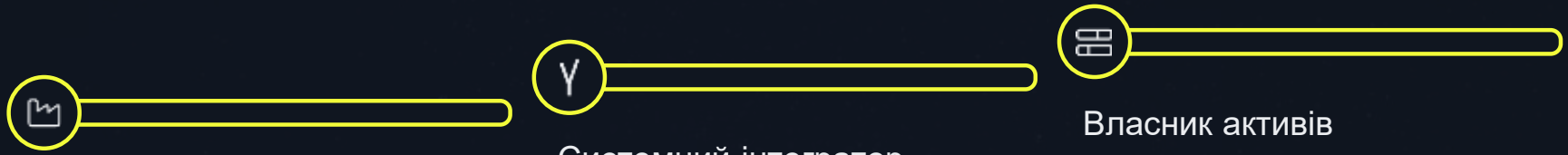
Строгий контроль доступу до документації архітектури систем, обмежуючи його лише уповноваженому персоналу на основі принципу "потреби знати"

2.4.2. Поділ обов'язків у кібербезпеці

Поділ обов'язків – це концепція, яка передбачає розподіл критично важливих завдань між кількома особами, щоб жодна людина не могла виконати шкідливу дію без участі або схвалення іншої.

Це допомагає мінімізувати потенційну шкоду від несанкціонованого доступу або помилок, забезпечуючи багатосторонній контроль над критичними операціями.

2.4.3. Ролі в стандарті IEC 62443



Постачальник продукції

Відповідає за розробку та тестування системи керування

Системний інтегратор

Несе відповідальність за інтеграцію та введення продукту в рішення щодо автоматизації

Власник активів

Відповідає за експлуатаційні можливості та технічне обслуговування за допомогою політик та процедур

2.4.4. Переваги розподілу відповідальності

Багатосторонній контроль

Забезпечує перевірку та баланс між різними сторонами у процесі безпеки

Запобігання концентрації влади

Не дозволяє занадто великій владі концентруватися в одних руках

Зниження ризиків

Мінімізує потенційну шкоду від внутрішніх загроз та випадкових помилок

2.4.5. Ключові рекомендації для впровадження

1

Планування та конфігурація

Ретельне планування розміщення міжмережевих екранів та IPS/IDS з урахуванням специфіки промислових протоколів

2

Постійний моніторинг

Забезпечення кваліфікованого персоналу для моніторингу систем безпеки та обробки інцидентів

3

Регулярне оновлення

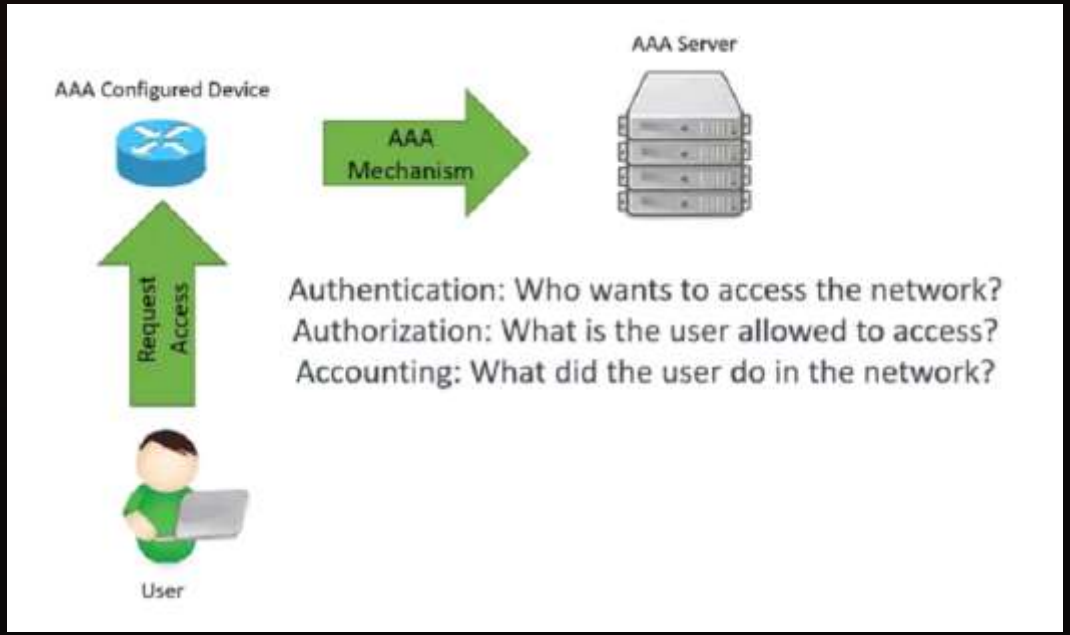
Підтримка актуальних сигнатур, патчів та документації систем безпеки

4

Інтеграція з SIEM

Об'єднання всіх систем безпеки в єдину платформу управління подіями

2.5. Висновки: Комплексний підхід до мережевої безпеки



Ефективний захист промислових систем ICS/SCADA вимагає комплексного підходу, що включає міжмережеві екрани, системи IPS/IDS, надійні механізми AAA, принцип найменших привілеїв та поділ обов'язків.

Успішне впровадження цих принципів залежить від ретельного планування, кваліфікованого персоналу, постійного моніторингу та регулярного оновлення всіх компонентів системи безпеки. Лише такий підхід може забезпечити надійний захист критично важливої промислової інфраструктури від сучасних кіберзагроз.

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!