УДК 004

А.Дабич, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ АУДИТУ БЕЗПЕКИ МЕРЕЖЕВИХ ICS/SCADA

У статті розроблено програмне забезпечення, яке призначено для системи аудиту безпеки мережевих ICS/SCADA. Метою розробки є дослідження та принципи побудови системи аудиту безпеки мережевих ICS/SCADA. Об'єктом дослідження є процес аудиту безпеки мережевих ICS/SCADA. Предметом дослідження є методи аудиту безпеки мережевих ICS/SCADA. Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи аудиту безпеки мережевих ICS/SCADA. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

аудит безпеки, мережа, ICS/SCADA

Постановка проблеми. Починаючи з кінця 60-х років минулого століття, промислові системи керування (Industrial Control System; ICS) з'явилися практично у всіх сферах, що мають відношення до сучасного життя: енергетика, промисловість, комунальні системи й інші області.

З моменту винаходу блокового цифрового контролера в 1968 році й до середини 90-х промислові системи керування були практично ізольовані й могли працювати з дуже обмеженим набором вхідних і вихідних даних із зовнішніх джерел.

Однак з появою дешевого устаткування, операційної системи Microsoft Windows, Active Directory і загальної стандартизації, сучасні корпоративні мережі стали одержувати й обробляти дані (а також виконувати інші безліч інших операцій) з мереж за межами традиційних ICS-мереж.

Незважаючи на те, що на даний момент уживає безліч зусиль по сегментації мереж пов'язаних з інформаційними й промисловими технологіями, границі дотепер залишаються розмитими, що доставляємо багато головного болю фахівцям з безпеки, що працює в багатьох індустріях.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи аудиту безпеки мережевих ICS/SCADA.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи аудиту безпеки мережевих ICS/SCADA.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем аудиту безпеки мережевих ICS/SCADA.
- Дослідження системи аудиту безпеки мережевих ICS/SCADA.
- Програмна реалізація системи аудиту безпеки мережевих ICS/SCADA.

Об'єктом дослідження є процес аудиту безпеки мережевих ICS/SCADA.

Предметом дослідження є методи аудиту безпеки мережевих ICS/SCADA.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Системи безпеки ICS/SCADA захищають промислові системи керування та мережі диспетчерського керування й збору даних, які керують 90% критичної інфраструктури в усьому світі, запобігаючи кібератак, які завдають середньої шкоди в розмірі 5,9 мільйона доларів на інцидент. Системи промислового керування керують електромережами, що обслуговують 7,8 мільярда людей, водоочисними спорудами, що переробляють 147 мільярдів галонів щодня, та виробничими підприємствами, що виробляють товарів на суму 14,2 трильйона доларів щорічно. Ці системи щодня стикаються з 2400 кібератак, причому успішні порушення призводять до збоїв у роботі, які тривають в середньому 23 дні, та загрожують безпеці людей у 47% інцидентів, що потребують комплексного захисту.

Ключові висновки:

– Системи ICS/SCADA контролюють 90% глобальної критичної інфраструктури, і на ці мережі щодня направляється 2400 кібератак.

– Порушення безпеки коштують організаціям в середньому 5,9 мільйона доларів США з 23-денними перебоями в роботі

– 73% систем ICS/SCADA мають невиправлені вразливості через вимоги цілодобової роботи

– Сегментація мережі зменшує успішність атак на 84% за умови правильного впровадження розділення IT/OT

– Відповідність таким стандартам, як NIST SP 800-82 та IEC 62443, запобігає 67% поширених векторів атак.

Безпека ICS/SCADA – це захисні заходи, технології та практики, що захищають промислові системи управління, мережі диспетчерського контролю та збору даних від кіберзагроз, фізичних атак та операційних збоїв. Безпека ICS/SCADA охоплює комплексний захист операційних технологій, що контролюють промислові процеси у виробничому, енергетичному, водному та транспортному секторах. ICS представляє ширшу категорію операційних технологій, що контролюють промислові процеси, тоді як SCADA спеціально контролює та контролює розподілені активи в різних географічних регіонах.

ІКС включає програмовані логічні контролери (ПЛК), розподілені системи керування (РСК) та людино-машинні інтерфейси (ХМІ), що керують 4,7 мільйонами промислових об'єктів по всьому світу. Системи SCADA збирають дані в режимі реального часу з 23 мільйонів віддалених терміналів (RTU) по всьому світу, що дозволяє операторам контролювати та керувати інфраструктурою, що охоплює тисячі миль. Зв'язок між ІКС та SCADA передбачає функціонування СКАДА як рівня нагляду над компонентами ІКС, що забезпечує централізовану видимість та контроль критично важливих операцій.

Як працює безпека ICS/SCADA?

Безпека ICS/SCADA працює за допомогою багаторівневих захисних механізмів, включаючи сегментацію мережі, спеціалізовані протоколи, системи виявлення вторгнень та контроль доступу, що захищають промислові мережі від кіберзагроз. Мережева архітектура реалізує рівні моделі Purdue, що відокремлюють корпоративні IT від операційних технологій за допомогою демілітаризованих зон та брандмауерів. Промислові протоколи, такі як Modbus, DNP3 та OPC, вимагають протокольно-залежних засобів контролю безпеки, що виявляють шкідливі команди та спроби несанкціонованого доступу.

Механізми безпеки включають односпрямовані шлюзи, що запобігають досягненню 99,9% мережевих атак критично важливих систем керування. Сегментація мережі створює ізольовані зони, зменшуючи поверхню атаки на 73% та обмежуючи порушення в певних областях. Системи виявлення вторгнень щодня відстежують 8,4 мільярда пакетів промислової мережі, виявляючи аномальну поведінку, що вказує на кібератаки або несправності системи.

Чому безпека ICS/SCADA є критично важливою для бізнес-операцій?

Безпека ICS/SCADA має вирішальне значення для бізнес-операцій, оскільки потенційні наслідки включають виробничі втрати в розмірі 1,4 мільйона доларів США

щогодини, інциденти безпеки, що щорічно впливають на 10 000 працівників, та збої в інфраструктурі, що порушують роботу мільйонів громадян. Кібератаки на промислові системи зросли на 140% між 2020 і 2024 роками, причому програми-вимагачі були спрямовані на 56% виробничих потужностей і спричиняли середній час простою 21 день. Передові постійні загрози з боку 37 угруповань національних держав активно націлені на критичну інфраструктуру з метою шпигунства та потенційних можливостей порушення роботи.

У 2010 році Stuxnet продемонстрував вразливість ICS, знищивши 1000 іранських центрифуг за допомогою складних маніпуляцій з ПЛК, одночасно відображаючи операторам нормальну роботу. У 2015 році шкідливе програмне забезпечення BlackEnergy порушило роботу українських енергомереж, залишивши 230 000 жителів без електроенергії протягом 6 годин у зимових умовах. У 2017 році шкідливе програмне забезпечення Triton/Trisis було спрямоване на системи безпеки, намагаючись відключити можливості аварійного вимкнення на нафтохімічних об'єктах, що потенційно могло спричинити вибухи.

Поширені вразливості присутні у 73% систем ICS/SCADA, включаючи застарілі технології, яким в середньому 19 років, і які не мають вбудованих функцій безпеки. Плоска мережева архітектура у 61% об'єктів дозволяє зловмисникам рухатися в горизонтальному напрямку після того, як зловмисники порушують захист периметра. Відсутність моніторингу в режимі реального часу у 43% промислових мереж дозволяє зловмисникам діяти непоміченими в середньому протягом 246 днів.

Як організації можуть подолати проблеми безпеки ICS/SCADA?

Організації можуть подолати проблеми безпеки ICS/SCADA, впроваджуючи спеціалізовані стратегії, що враховують унікальні операційні обмеження, включаючи вимоги до цілодобової доступності, 20-річний життєвий цикл обладнання та критично важливі для безпеки операції, які не терплять перебоїв. Обмеження щодо виправлень впливають на 82% середовищ ICS, де системи не можна вивести з режиму автономного режиму для оновлень, що вимагає компенсуючих елементів керування, таких як віртуальне виправлення та мережева ізоляція. Застарілі системи, несумісні із сучасними інструментами безпеки, вимагають використання технологій-обгорток, що забезпечують захист без модифікації оригінального обладнання.

Спеціалізовані інструменти безпеки для OT, розроблені для промислових протоколів та вимог реального часу, захищають системи, не впливаючи на роботу. Рішення для пасивного моніторингу аналізують мережевий трафік без надсилання пакетів, запобігаючи випадковим збоям у роботі системи, які впливають на 11% активних сканерів. Інструменти інвентаризації активів виявляють 100% підключених пристроїв, включаючи 31%, які зазвичай невідомі операторам, завдяки комплексним процесам виявлення.

Програми навчання персоналу навчають 2,3 мільйона промислових операторів у всьому світі ризикам кібербезпеки та процедурам реагування. Інженерні команди проходять навчання з безпеки операційних систем, що охоплює безпечне програмування для ПЛК, посилення мережевої архітектури та реагування на інциденти. Перехресне навчання між командами IT та операційних систем усуває прогалини в знаннях, і 89% успішних програм потребують управління культурними змінами.

Поширені загрози для ICS/SCADA

Поширеними загрозами для ICS/SCADA є цільове шкідливе програмне забезпечення, дії інсайдерів, компрометація ланцюгів поставок, мережеві атаки та зловживання фізичним доступом, що завдає середньої шкоди в розмірі 5,9 мільйона доларів США за інцидент. Ці загрози використовують вразливості операційних технологій за допомогою складних методів атак, розроблених спеціально для промислового середовища.

Шкідливе програмне забезпечення та програми-вимагачі, спрямовані на SCADA

Шкідливе програмне забезпечення та програми-вимагачі атакують системи SCADA через спеціалізовані варіанти, розроблені для промислових процесів, причому кількість атак зросла на 2000% з 2010 року. Атаки програм-вимагачів на промислові об'єкти вимагають

середніх платежів у розмірі 2,3 мільйона доларів США, шифруючи HMI та бази даних історії, критично важливі для операцій. Програма-вимагач EKANS спеціально націлена на промислові системи управління, перевіряючи та завершуючи 64 процеси, специфічні для ICS, до початку шифрування. Методи збереження шкідливого програмного забезпечення використовують інженерні робочі станції, причому 43% атак відбуваються із заражених ноутбуків постачальників під час технічного обслуговування.

Внутрішні загрози та людські помилки

Внутрішні загрози та ризики людських помилок становлять 34% інцидентів безпеки ICS, причому зловмисники завдають збитків у середньому на суму 4,7 мільйона доларів США через саботаж або крадіжку даних. Внутрішні загрози включають співробітників, підрядників та постачальників з доступом до систем, що становить 67% ризиків безпеки, часто без навчання з питань безпеки. Людська помилка спричиняє 52% інцидентів безпеки ICS, включаючи неправильну конфігурацію, переходи за фішинговими посиланнями та випадкове відключення засобів контролю безпеки. Моніторинг привілейованих користувачів виявляє 89% внутрішніх загроз, зменшуючи вплив інцидентів на 71% завдяки ранньому виявленню та реагуванню.

Компроміси в ланцюжку поставок

Компрометації ланцюгів поставок впливають на ICS/SCADA через атаки, спрямовані на постачальників та інтеграторів, які зросли на 430% між 2020 і 2024 роками, торкнувшись тисяч клієнтів нижчої ланки. Атаки на ланцюги поставок, такі як SolarWinds, вплинули на 18 000 організацій, включаючи операторів критичної інфраструктури, які керують системами живлення та водопостачання. Апаратні імплантати, виявлені у 0,3% поставок промислового обладнання, забезпечують постійний бекдор-доступ, що витримує оновлення прошивки та скидання системи. Вразливості сторонніх компонентів впливають на 73% пристроїв ICS через спільні бібліотеки та вбудовані системи, що вимагають комплексної безпеки ланцюга поставок.

Мережева атака

Методи мережевих атак включають атаки типу «людина посередині», які перехоплюють та змінюють 31% незашифрованого зв'язку ICS, маніпулюючи показаннями датчиків та командами керування. Атаки типу «відмова в обслуговуванні», спрямовані на промислові мережі, спричиняють середній час простою 14 годин, що коштує 940 000 доларів США за інцидент через втрати виробництва. Експлуатація протоколів використовує незахищені за своєю природою промислові протоколи, 67% з яких не мають можливостей автентифікації або шифрування. Мережева розвідка виявляє вразливі системи у 94% промислових мереж протягом 72 годин після першого доступу.

Експлуатація фізичного доступу

Фізичний доступ дозволяє здійснювати експлуатацію шляхом обходу засобів контролю безпеки мережі, причому 23% об'єктів мають недостатній фізичний захист критично важливих систем керування. Атаки на основі USB через знімні носії залишаються ефективними у 61% систем з обмеженим доступом, поширюючи шкідливе програмне забезпечення по ізольованих мережах. Введення несанкціонованих пристроїв, включаючи точки бездротового доступу, щорічно ставить під загрозу 17% захищених об'єктів, створюючи несанкціоновані мережеві мости. Фізичне втручання в датчики та виконавчі механізми призводить до збоїв у процесах, які не виявляються системами кібермоніторингу, зосередженими на мережевому трафіку.

Що таке стратегії та найкращі практики кібербезпеки ICS/SCADA?

Стратегії кібербезпеки ICS/SCADA – це підходи до глибокого захисту, що поєднують сегментацію мережі, принципи нульової довіри, безпечний віддалений доступ, безперервний моніторинг та планування реагування на інциденти, що зменшує успішність атак на 84%. Ці стратегії враховують унікальні вимоги до операційних технологій, зберігаючи при цьому доступність та безпеку системи.

Як сегментація мережі захищає ICS/SCADA?

Сегментація мережі захищає ICS/SCADA, розділяючи IT- та OT-середовища за допомогою брандмауерів, зменшуючи успішність горизонтального переміщення на 91% під час порушень. Сегментація мережі реалізує модель Пердью, створюючи ієрархічні зони з контрольованим зв'язком між рівнями, що містять 87% атак у початкових зонах компрометації. Мікросегментація в OT-мережах ізолює критичні системи, обмежуючи радіус вибуху під час виникнення інцидентів. Розгортання DMZ між IT- та OT-мережами фільтрує 4,7 мільярда спроб підключення щодня, блокуючи 99,3% несанкціонованого трафіку.

Як принципи нульової довіри застосовуються до ICS/SCADA?

Принципи нульової довіри застосовуються до ICS/SCADA шляхом перевірки кожного з'єднання незалежно від джерела, що зменшує несанкціонований доступ на 94% завдяки постійній перевірці. Архітектура нульової довіри для ICS/SCADA перевіряє всіх користувачів, пристрої та програми, запобігаючи 78% атак на основі облікових даних. Доступ з мінімальними привілеями обмежує користувачів мінімально необхідними дозволами, що містить пошкодження від скомпрометованих облікових записів. Безперервна перевірка відстежує моделі поведінки, виявляючи аномалії у 97% сценаріїв внутрішніх загроз.

Що таке протоколи безпечного віддаленого доступу?

Безпечні протоколи віддаленого доступу замінюють 73% вразливих VPN-з’єднань на зашифровані сервери переходів та рішення для керування привілейованим доступом. Багатофакторна автентифікація запобігає 99,9% автоматизованих атак на портали віддаленого доступу, що використовуються постачальниками та підрядниками. Запис та моніторинг сеансів відстежують усі віддалені дії, надаючи судово-медичні докази для 100% віддалених сеансів. Контроль доступу на основі часу обмежує вікна з’єднань, зменшуючи вразливість на 67% порівняно з методами постійного доступу.

Як працюють безперервний моніторинг та виявлення аномалій?

Безперервний моніторинг та виявлення аномалій працюють шляхом аналізу 12 мільярдів подій мережі ICS щодня, виявляючи загрози протягом 4 хвилин після початкової активності. Безперервний моніторинг використовує алгоритми машинного навчання для базової оцінки нормальної роботи, а потім виявляє відхилення з точністю 94% та рівнем хибних спрацьовувань 0,3%. Моніторинг активів відстежує зміни конфігурації, виявляючи несанкціоновані модифікації, щомісяця впливають на 31% пристроїв ICS. Моніторинг змінних процесу виявляє маніпулювання показаннями датчиків та командами керування, що вказують на кіберфізичні атаки.

Чому важливі планування реагування на інциденти та проведення навчальних заходів?

Планування реагування на інциденти та практичні навчання є важливими, оскільки плани, специфічні для ICS/SCADA, скорочують час відновлення на 73% порівняно із загальними процедурами реагування на IT. Плани реагування на інциденти враховують унікальні операційні вимоги, надаючи пріоритет критично важливим для безпеки системам та підтримуючи роботу під час інцидентів. Практичні навчання, що проводяться щоквартально, покращують координацію команди, виявляючи прогалини в процесах у 89% симуляцій. Посібники з поширених сценаріїв, включаючи атаки програм-вимагачів та системи безпеки, допомагають у прийнятті рішень, що запобігають паніці.

Що таке стандарти безпеки ICS/SCADA та рамки відповідності?

Стандарти безпеки та структури відповідності ICS/SCADA є базовими вимогами та найкращими практиками для організацій, які дотримуються структур, що зменшує кількість інцидентів безпеки на 67% порівняно з об'єктами, що не відповідають вимогам. Ці стандарти враховують унікальні вимоги до операційних технологій, включаючи продуктивність у режимі реального часу, доступність та безпеку.

Стандарт NIST SP 800-82 надає комплексні рекомендації щодо безпеки ICS, яких прийняли 43% операторів критичної інфраструктури США, враховуючи унікальні вимоги до

240 засобів контролю безпеки. Впровадження зменшує вразливості на 71% завдяки систематичному управлінню ризиками та вибору засобів контролю безпеки. Серія ISA/IEC 62443 представляє міжнародні консенсусні стандарти безпеки промислової автоматизації, що впроваджені в 67 країнах.

Стандарти NERC CIP вимагають від 3000 північноамериканських операторів оптових електричних систем дотримання 45 вимог за 11 стандартами. Порушення призводять до щоденних штрафів у розмірі 1 мільйона доларів, тоді як впровадження запобігає 73% поширених векторів атак за допомогою необхідних заходів контролю. Керівні принципи CISA містять галузеві рекомендації щодо безпеки ICS для 16 секторів критичної інфраструктури, що дозволяє 4700 організаціям отримувати інформацію про загрози.

Специфічні для GCC правила стосуються регіональних вимог безпеки ICS/SCADA, а структура NESA OAE передбачає 33 елементи керування для операторів критичної інфраструктури. Стандарти NCSA Катару вимагають оцінки безпеки ICS для національної інфраструктури, що виявляє вразливості у 94% оцінених систем. Регіональне співробітництво через GCC-CERT обмінюється інформацією про загрози між державами-членами, запобігаючи транскордонним кіберінцидентам.

Незважаючи на важливість правильної ізоляції й інтерес до теми, пов'язаної з експертизою мереж, в інтернеті мало інформації стосовно цього питання. У цьому розділі будуть освітлені найпоширеніші проблеми, пов'язані з ізоляцією мереж, з якими ми зіштовхувалися під час попередніх експертиз. Сподіваємося, що ця інформація допоможе пентестерам глибше поринути в цю тему, а співробітникам, відповідальним за безпеку, відкриє завісу методів, якими користуються зловмисники для одержання доступу до нижніх шарів мережі керування виробничими процесами з боку корпоративної мережі.

Тестування сегрегації мережі звичайно складається з декількох кроків:

– Збір інформації.
– Ідентифікація місця проникнення.
– Доступ до сегрегованої мережі.

Збір інформації

Збір інформації в основному спрямований на ідентифікацію будь-яких незахищених даних, зв'язаних мережею керування виробничими процесами. Ця інформація може розкрити деталі про мережу керування, які допоможуть зловмисникові одержати доступ. Звичайно тут мається на увазі наступне:

– Інформація про персонал, що має відношення до керування процесами -технологи, оператори, IT-персонал і інші ключові люди звичайно володіють конфіденційною інформацією про мережу керування виробничими процесами. Пошук в Active Directory по співробітниках, які виконують вищезгадані ролі, може допомогти в ідентифікації імен робочих станцій і спільно використовуваних мережних ресурсах (кулях), до яких є доступ. Уже цей крок значно скорочує обсяг аналізованих даних і загальна кількість зусиль, необхідних для одержання доступу до мережі керування, оскільки в цьому випадку увага буде зосереджено тільки на певних хостах і кулях.

– Мережні діаграми й проектна документація – ця інформація може допомогти зловмисникові зрозуміти механізми роботи мережі керування процесами на фундаментальному рівні, а також виявити імена хостів і IP-адреси як відправні крапки для наступного збору відомостей. Більше того, в ідеальній ситуації мережна документація може дати повну картину керування, що відбувається в мережі, виробничими процесами й допомогти виявити хости, які потрібно атакувати в першу чергу. Після ідентифікації файлових серверів у корпоративній мережі й інформаційних репозитаріїв (наприклад, SharePoint) мережна документація звичайно шукається у файлах VSD, PDF і DOC / DOCX, що перебувають у директоріях або кулях, що мають відношення до відповідних процесів.

– Документація на мережу керування процесами -ця інформація може містити деталі офіційних процедур, пов'язаних з вилученим доступом, інструкції про авторизацію на хости, що мають відношення до виробничих процесів, і дані про технології (використовуваних і

невикористовуваних). У багатьох випадках, у подібній документації втримується надзвичайно важлива й конфіденційна інформація (наприклад, логіни й паролі), що є безцінною під час експертизи сегрегації мережі. Ця документація може перебувати усередині IT-куля й директорій або іноді в папках і кулях, що мають відношення безпосередньо до виробничих процесів.

– Мережні пристрої й бекапи систем – конфігураційні файли файервола, роутера й світча, які перебувають усередині резервної копії в корпоративній мережі, часто допомагають побудувати оптимальну схему проникнення в мережу керування. При вивченні конфігурації мережних пристроїв можна виявити хости в корпоративній мережі, до яких дозволений вилучений доступ через протоколи RDP, VNC і SSH. Якщо в корпоративній мережі перебувають бекапи систем, пов'язаних з керуванням процесами, то із цих даних можна легко витягти хеші й інші конфіденційні відомості. Ця інформація часто може бути отримана через додатки для IT-керування або мережного резервного копіювання, а також у корпоративні або мережних IT-кулях.

Ідентифікація місця проникнення

Один із ключових моментів на етапі збору інформації – ідентифікація існуючих місць проникнення в мережу керування виробничими процесами з корпоративної мережі. У більшості ситуацій можна знайти наступні типи місць проникнення:

– Jump-сервер (jumpbox) / Термінальний сервер- Доступ до мережі керування процесами з корпоративної мережі часто дозволений через хост, що функціонує як jump-сервер (або jump box). Звичайно вилучений доступ здійснюється через протоколи RDP, VNC і SSH. Хоча іноді використовуються додатки для віртуалізації робітників столів на зразок Citrix. Організації, що приділяють мірам безпеки особлива увага, часто використовують рішення, що підтримують багатофакторну автентифікацію під час вилученого доступу.

У документації часто описуються офіційні процедури для вилученого доступу до мережі керування виробничими процесами. Jump-сервера або термінальних служб також можуть бути ідентифіковані за допомогою аналізу мережних діаграм або конфігураційних файлів файервола для хостів, яким дозволені з'єднання з корпоративної мережі через стандартні порти вилученого доступу. Дослідження робочих станцій персоналу в корпоративній мережі, що має відношення до керування процесами, часто є ефективним способом ідентифікації jump-серверів і протоколу, використовуваного для вилученого доступу:

– VPN-доступ – Обраним користувачам, що звичайно мають відношення до керування процесами, може бути дозволений прямій VPN-доступ з метою вилученого керування мережею. Так само як і у випадку з jump-серверами тут може використовуватися багатофакторна автентифікація.

Іноді для цих користувачів може бути створена окрема група. Вивчення імен і опису груп, у які входять ключові співробітники, що мають відношення до виробничих процесів, звичайно дозволяє виявити групу користувачів, у яких є VPN-доступ. Далі починається дослідження робочих станцій цих користувачів на предмет присутності VPN-інтерфейсів або додатків, а також активних з'єднань до мережі керування виробничими процесами. Ці робочі станції можуть використовуватися як міст до мережі керування.

– Дводомні хости – У типовій мережі, пов'язаної з керуванням виробничими процесами, трохи хостів можуть бути зконфігурованим як дводомні або за допомогою додаткових правил файервола, які дозволяють доступ до мережі керування. Звичайно в цю категорію попадають сервера, що зберігають архівні дані, використовувані з метою аналізу й поліпшення продуктивності виробничих процесів. Одержання доступу до цим хостам часто дає прямий доступ до мережі керування виробничими процесами без необхідності використання офіційних процедур вилученого доступу. Навіть якщо архівні сервера не дають розширеного доступу до мережі керування, дослідження активних з'єднань допомагає виявити діапазони цільових IP-адрес.

Найбільш надійний спосіб пошуку хостів з архівними даними – аналіз мережної документації й діаграм. Крім того, незайвим буде звернути увагу на імена хостів (архівні хости часто мають імена “HI”, “HIS”, “HIST” або щось у такому дусі). Можна спробувати посканувати порти, однак це завдання ускладнюється тим, що не існує єдиного стандарту портів, використовуваних виробниками. Хоча багато організацій використовують архівні сервера на базі системи OSISoft PI, які можна виявити за допомогою сканування найпоширеніших портів, пов'язаних із цим програмним забезпеченням (https://techsupport.osisoft.com/troubleshooting/kb/2820osi8). У цілому, якщо виробник системи керування відомий або виявлений у процесі аналізу, то далі вивчається загальнодоступна документація на предмет використання розповсюджених портів для наступного сканування в корпоративній мережі.

Ще один ефективний метод виявлення дводомних хостів – обстеження корпоративної мережі за допомогою виконання вилучених команд певним чином (наприклад, WMI або PSExec) і добування активних з'єднань, мережних інтерфейсів і таблиць маршрутизації. Ці дані потім використовуються для пошуку хостів, що мають доступ до мережі керування виробничими процесами. Хоча цей метод створює багато шуму, забирає багато часу й може видавати величезні обсяги інформації для парсингу, особливо в більших мережах. З іншого боку, фільтрація по отриманим раніше діапазонах IP-адрес, які використовуються мережею керування, значно спрощує завдання.

Доступ до сегрегованої мережі

Після одержання потенційних місць проникнення в мережу керування виробничими процесами наступний крок – дослідження кожного місця на предмет присутності розповсюджених уразливостей з метою одержання доступу до мережі керування. Нижче перераховані найпоширеніші проблеми, які були виявлені під час експертизи різних мереж.

– Небезпечні паролі – Паролі є серйозною проблемою для співробітників, відповідальних за безпеку мережі керування виробничими процесами, з кількох причин. Основна проблема полягає в складності мотивації інженерів і інших користувачів, у яких є доступ до мережі керування, до використання стійких паролів. Найчастіше використовуються ті самі паролі й у корпоративній мережі й у мережі керування, оскільки користувачі не бажають управляти набором паролів і вважають, що ризик злому мережі ніщо малий. Після компрометування корпоративної мережі й злому / одержання паролів ключових співробітників, ті ж самі паролі можуть використовуватися для доступу до мережі керування виробничими процесами через раніше отримані місця проникнення.

Дуже часто використовуються стандартні або слабкі паролі, які встановлені виробником за замовчуванням. Ці паролі ніколи не міняються, щоб уникнути проблем, пов'язаних з відхиленням від стандартної конфігурації. Часто імена користувачів і паролів збігаються (наприклад, operator: operator, manager: manager, supervisor: supervisor) або використовуються варіації ім'я виробника (наприклад, Administrator: siemens).

Ситуація погіршується ще тим, що політики блокування паролів, використовуваних у виробничих процесах, звичайно не визначені через запобігання випадкових блокувань, які можуть привести до проблем або зупинки всього процесу. Хоча ця ідея й має право на життя, але з іншої сторони зловмисникові відкриваються можливості для прямого підбора облікових записів. Ця проблема в комбінації з попередніми (слабкі й повторно використовувані паролі) робить атаку по переборі надзвичайно ефективної при спробі одержання доступу до мережі керування виробничими процесами.

– Зберігання паролів у відкритому виді – Облікові записи, використовувані при керуванні технологічними процесами, часто втримуються в документації. Будь-які репозиторії, де зберігається документація мережі керування виробничими процесами, повинні бути досліджені на етапі збору інформації при експертизі сегрегації мережі. Будь-яка знайдена документація повинна бути проаналізована на предмет паролів, використовуваних у місцях проникнення.

– Домен корпоративної мережі підключений до мережі керування – У випадку присутності в корпоративній мережі дводомних хостів або робітників станцій з VPN-доступом ці хости звичайно приєднані до домену в Active Directory. Відповідно, стає можливим одержання доступу до цим хостам прямо за допомогою високопривілійованих облікових записів, використовуваних в Active Directory з боку корпоративної мережі (наприклад, за допомогою облікового запису адміністратора домена). В організаціях, де безпеки приділяється особлива увага, уживають додаткові кроки по обмеженню доступу до цим хостам тільки для певних користувачів або груп. Хоча якщо корпоративна мережа скомпрометована, те досить просто знайти потрібних користувачів і витягти паролі з пам'яті.

– Відкриті уразливі служби – У місцях проникнення можуть використовуватися додаткові служби (наприклад, бази даних або веб-застосунка), уразливі до найпоширеніших атак. Кожний хост, у якого є доступ до мережі керування виробничими процесами, повинен бути просканован на предмет присутності неврахованих служб. У випадку знаходження подібних служб потрібно провести аналіз на предмет наявності уразливостей або розповсюджених помилок у конфігурації, які можуть стати причиною компрометування всього хоста.

Рисунок 1 – Структурна схема системи

Якщо ви коли-або, виконуючи пентести ICS-інфраструктури, зштовхнетеся з однієї з наступних ситуацій, негайно рапортуйте про критичну проблему:

– У корпоративній мережі виявлений трафік Modbus/DNP3.

– З корпоративної мережі є доступ до людино-машинного інтерфейсу (HMI) із правами не тільки на читання.

– Пінгування ядерного реактора за допомогою NMAP приводить до необоротних наслідків.

Сподіваємося, що остання ситуація з вами ніколи не трапиться. У противному випадку, бажаємо вам залишитися цілим і непошкодженим.

Незважаючи на те, що навколо нас багато чого залежить від ICS-технологій, існує явний недолік інформації щодо безпеки подібних систем.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів аудиту безпеки мережевих ICS/SCADA. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем аудиту безпеки мережевих ICS/SCADA.

– Досліджена система аудиту безпеки мережевих ICS/SCADA.

– На основі отриманих результатів досліджень створена програмна реалізація системи аудиту безпеки мережевих ICS/SCADA. Розроблені алгоритми дозволяють успішно вирішувати завдання аудиту безпеки мережевих ICS/SCADA. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Вінтенко Б.Ю., Миронець І.В., Смірнов О.А. «Модель комп’ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». IV Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2025)» м.Черкаси 25 листопада 2025 року – Черкаси: ЧДТУ.– 2025. – С.101-103.
2. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». Cybersecurity Defensive Walls in Edge Computing, 2025. pp. 21-61.
3. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С. 413-427, 2025.
4. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С.195-208, 2025.
5. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
6. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
7. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
8. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп’ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
9. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». International Review on Modelling and Simulations 18 (1), 2025. pp. 32-42.
10. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп’ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». Центральноукраїнський науковий вісник. Технічні науки. 2025. Вип. 11(42), ч. ІІ. С.52-62.
11. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології”, м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
12. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Конопліцька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об’єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 6-26.
13. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова

Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
14. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
16. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
17. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
18. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
19. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 3(73), С. 155-166.
20. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
21. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
22. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
23. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
24. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
25. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
26. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
27. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
28. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
29. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
30. Smirnov O., Kuznetsov A., Pushkar’ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
31. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.