МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
WARSAW UNIVERSITY OF LIFE SCIENCES
PRZEMYSLOWY INSTYTUT AUTOMATYKI I POMIAROW

Факультет автоматизації і комп'ютерних систем

IV Міжнародна науково-технічна
Internet-конференція

IV International Scientific Internet-Conference

«Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами»

"Modern methods, information, software and technical support of control systems for organizational, technical and technological complexes"

22 листопада 2017 рік

КИЇВ НУХТ 2017

УДК 004.4

Аналіз безпеки систем ICS / SCADA

І.В. Бокоч, С.М. Швед

Національний університет харчових технологій

Системи SCADA / ICS вимагають особливої уваги до питань інформаційної безпеки, так як потенційні кібератаки і зловживання співробітників можуть привести до катастрофічних наслідків, починаючи від втрати конфіденційної інформації і аж до порушення технологічного процесу і великих аварій. [4]

Не секрет, що пристрої, що використовуються в системах управління виробничими процесами, уразливі до атак. Ця гіпотеза підтверджується безліччю досліджень і навіть є предметом незліченних дискусій та семінарів. На жаль, персонал, відповідальний за безпеку цих мереж, часто стикається з різними труднощами, головна з яких - конфігурація і регулярне оновлення систем без необхідності зупиняти робочий процес. Крім того, фахівці часто безуспішно намагаються впровадити ідею про безпеку в голови людей, що беруть участь в різних технологічних процесах, які відносяться до цього питання скоріше як до непотрібної нісенітниці. Особливо в нижніх шарах мережі, пов'язаної з управлінням виробничими процесами. Як вирішення цієї проблеми, більша увага стала приділятися сегрегуванню (ізоляції) мережі і створення безпечних зон для систем управління особливо важливими і критичними процесами. Тобто стали зміцнюватися кордони між корпоративною мережею та системами SCADA / мережами управління процесами, а також стали посилюватися права доступу.

Загальне правило: оцінка сегрегації мережі виконується з тим припущенням, що зловмисникові вже вдалося скомпрометувати корпоративну мережу для того, щоб зімітувати реальний сценарій атаки. Зазвичай або дається доступ з правами адміністратора домену або експертиза виконується спільно з пентестом корпоративної мережі.

Тестування сегрегації мережі зазвичай складається з декількох кроків:

Збір інформації.

Ідентифікація місця проникнення.

Доступ до сегрегованої мережі.

Збір інформації [1]

Незважаючи на те, що підготовлений зловмисник може отримати прямий доступ до ICS-середовища через соціальну інженерію або фізичну атаку, швидше за все злом буде здійснено через корпоративну мережу за допомогою експлуатації достовірних з'єднань до SCADA-серверів і людино-машинним інтерфейсів. Навіть якщо зловмисникові не вдасться отримати доступ до конфіденційних даних або нанести яку іншу шкоду, штрафи, розслідування і претензії регулятора, пов'язані зі зломом ICS-середовища, можуть привести до катастрофічних наслідків для організації.[3]

Спочатку технологія ICS проектувалася без урахування аутентифікації,

шифрування, утиліт проти шкідників, фаєрволів та інших захисних механізмів, і, відповідно, ці системи не враховують сучасних реалій. Наприклад, одна з традиційних стратегій, що знижують IT-ризики, - своєчасна установка оновлень в уразливих системах. У той час як в сучасних IT-системах час простою під час оновлень прагне до нуля, в більшості ICS-систем виникають значні витрати і зниження продуктивності. Крім того, на відміну від традиційних IT-систем, неправильне оновлення ICS-пристрою може призвести до катастрофічних наслідків: заражені продукти харчування, відключення електрики, серйозні травми або навіть смерть.[2]

Один з ключових моментів на етапі збору інформації - ідентифікація існуючих місць проникнення в мережу управління виробничими процесами з корпоративної мережі. Мережі, пов'язані з управлінням процесами, рідко повністю ізольовані через те, що можуть перебувати на значній відстані або в несприятливих виробничих середовищах. Як підсумок, для управління подібними пристроями і системами часто використовуються протоколи віддаленого доступу.[1]

Хоча можна вважати, що фахівці з області ІБ на промислових підприємствах обізнані про сучасні кіберзагрози, їх розуміння суті цих загроз і необхідних контрзаходів залишає бажати кращого. На даний момент стратегії в області кібербезпеки в основному непослідовні: компанії впроваджують рішення, але не приділяють належної уваги політикам інформаційної безпеки, навчанню персоналу і грамотним налаштуванням використовуваного ПЗ.[3]

Для вирішення даної проблеми промисловим організаціям треба інвестувати кошти в своїх співробітників - щоб вони більше знали про проблеми інформаційної безпеки і були більш кіберграмотними. Недостатній практичний досвід можна компенсувати - наприклад, залучивши спеціалізовані сторонні команди, які розбираються в специфіці промислової кібербезпеки.

Крім того, слід враховувати, що рішення, розроблені спеціально для даного сектора, забезпечують більш ефективний захист, ніж універсальні програми, які, як було виявлено, як мінімум в 50% випадках залишають проломи системах АСУ ТП незакритими.

Література

1. Анализ безопасности систем ICS/SCADA: Типичный подход [Електронний ресурс]/ офіційний сайт. – Режим доступу: http://www.securitylab.ru/analytics/487978.php – Назва з екрану.

2. Введение в безопасность систем ICS/SCADA [Електронний ресурс]/ офіційний сайт. – Режим доступу: http://www.securitylab.ru/analytics/487977.php – Назва з екрану.

3. Кибербезопасность АСУ ТП: вести с передовой [Електронний ресурс]/ офіційний сайт. – Режим доступу: https://www.kaspersky.ru/blog/ics-report-2017/17812/ – Назва з екрану.

4. КІБЕРБЕЗПЕКА [Електронний ресурс]/ офіційний сайт. – Режим доступу: https://www.datas-tech.com/services/information_security_solutions – Назва з екрану.