УДК 004.056

МОДЕЛЬ АРХИТЕКТУРЫ HONEYPOT СИСТЕМЫ ДЛЯ ИЗУЧЕНИЯ ВЕКТОРА АТАК НА УСТРОЙСТВА IIOT

Баринова Я.В. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Менщиков А.А.
(Университет ИТМО)

В работе рассмотрены ключевые возможности предложенной архитектуры honeypot, приведено функциональное описание основных компонентов системы. Предлагаемая архитектура впоследствии может быть применима для обеспечения информационной безопасности предприятий и изучения атак на устройства промышленных Интернет вещей (IIoT).

Введение. В результате стремительного развития технологического сектора возрастает количество устройств промышленного контроля (IIoT) в критически важной инфраструктуре, что приводит к увеличению числа потенциальных кибератак.
Одним из способов прогнозирования и предотвращения атак на устройства промышленной инфраструктуры может выступать технология ловушек (honeypot). Технология позволяет провести анализ поведения киберпреступника в сети и определить, каким образом могут быть нанесены удары по существующим объектам безопасности. Собранные данные о сетевом трафике впоследствии могут быть изучены для разработки актуальных средств противодействия.

Основная часть. На данный момент большинство honeypot решений нацелены на изучение инцидентов персональных устройств Интернет вещей, которые не способны обнаружить вектор атак, применяемый на промышленные системы.
На первом этапе работы проводится анализ существующих ловушек для устройств Интернет вещей и составляются требования к системе, предназначенной для исследования поведения злоумышленника после его проникновения внутрь it-инфраструктуры предприятия. Далее, на основе проведенного анализа, строится модель honeypot системы, направленная на решение следующих задач:

- выявление ранее неизвестных уязвимостей в промышленной сети
- выявление ранее неизвестного программного обеспечения
- пошаговое изучение действий киберпреступников в системе
- сбор сведений об используемой инфраструктуре злоумышленника

В предложенной архитектуре honeypot-системы используются взаимосвязанные функциональные блоки, такие как система верификации, сервер nginx, сервер MySQL, контроллер (модуль извлечения записей логов и предварительной предобработки), анализатор (модуль, осуществляющий аналитическую обработку данных в хранилище).

Выводы. Предложенная архитектура honeypot-системы может снизить количество ложных срабатываний, выдаваемых другими средствами защиты информации, внедренными в промышленную инфраструктуру, такими как IDS/IPS-системы. Это является основным преимуществом honeypot делает чрезвычайно эффективным использование таких систем для обнаружения атак. В дальнейшем запланировано проведение экспериментов в лабораторных условиях предложенной архитектуры исследовательской honeypot-системы.

Баринова Я.В. (автор)

Менщиков А.А. (научный руководитель)