УДК 004.056.53

Использование систем поддержки принятия решений при определении целевого профиля безопасности в соответствии с IoT Security Maturity Model

Автор - Рыбаков С.Д. (Университет ИТМО)

Научный руководитель – Рудина Екатерина Александровна, ведущий системный аналитик АО “Лаборатория Касперского”, к.т.н.

В связи с развитием компьютерной техники, а особенно таких ее областей как Интернет вещей и Индустрия 4.0, все более важным становится вопрос обеспечения кибербезопасности ИТ систем и сетей. Теперь этот вопрос связан не только с конфиденциальностью и целостностью данных пользователей, но и с возможными физическими последствиями инцидентов безопасности для промышленных объектов, для общественного и личного транспорта, для любых систем равно в повседневной жизни и в критически важных областях человеческой деятельности. Последствия атак могут быть непредсказуемыми или тщательно рассчитанными. Например, червь Slammer случайно отключил всю Южную Корею от глобальной сети Интернет более, чем на три часа, а червь StuxNet откинул в развитии Иранскую ядерную программу на несколько лет назад путем намеренного физического разрушения центрифуг обогащения уранового топлива.

Оценка необходимости обеспечения безопасности у различных организаций будет всегда разной. Даже при схожих рисках последствия возможных инцидентов для одних компаний могут быть более значимыми, чем для других. Зрелая с точки зрения безопасности система характеризуется достаточным набором мер защиты, которые в то же самое время не препятствуют ее работе в нормальном режиме. При этом определения «достаточности защиты», «нормального режима» и понятия «препятствовать» для каждой системы свои.

Для упорядочивания и категоризации способов обеспечения безопасности конкретной системы с учетом ее ограничений и особенностей участники Консорциума промышленного интернета (Industrial Internet Consortium) разработали модель зрелости безопасности интернета вещей (IoT Security Maturity Model). Конечная цель модели зрелости безопасности (IIC IoT Security Maturity Model, IoT SMM) – обеспечить соответствие способов защиты от киберугроз реальным бизнес-потребностям. Задача - сформировать конкретное описание состояния «достаточной безопасности» для заказчика, помочь ему сфокусироваться на наилучших способах достижения этого состояния и определить соответствующие меры защиты. Это описание состояния носит название целевого профиля зрелости безопасности (Security Maturity Profile). Руководство по применению модели включает руководство достижению целевого профиля зрелости безопасности. Таким образом, модель помогает инвестировать в механизмы и меры безопасности, которые наилучшим образом отвечают бизнес-потребностям.

Архитектурой выбора и ядром модели зрелости безопасности интернета вещей является иерархия практик обеспечения безопасности (security practices). Практикой обеспечения безопасности, к примеру, является реализация контроля доступа, защита

данных при их хранении и передаче или управление обновлениями безопасности. Системный подход к выбору вариантов защиты поддерживается группированием практик по ожидаемому эффекту от их применения. Для максимального упрощения процесса выбора группы практик делятся на три домена на верхнем уровне (управления безопасностью и организационные меры; обеспечение безопасности в силу конструкции; укрепление безопасности), каждый из которых включает по три поддомена, содержащих две конкретные практики.

При практическом применении модели могут возникнуть такие ситуации, как потребность определения текущего уровня безопасности системы в привычном бизнесу, например, процентном виде, установления порядка очередности принимаемых мер, или же необходимость заменить одну практику другой/другими. В этом случае на помощь приходят системы поддержки принятия решений, которые опираясь на входные данные и объективный анализ предметной деятельности позволяют в соответствии с определенными методами принятия решений быстро и точно ответить на данные вопросы.

Один из возможных и наиболее подходящий метод принятия решений - метод анализа иерархий (МАИ), разработанный математиком Томасом Л. Саати, поскольку именно он позволяет понятным и рациональным образом структурировать сложную проблему принятия решений в виде иерархии, сравнить и выполнить количественную оценку альтернативных вариантов решения, а также является достаточно изученным и имеет несколько различных модификаций, потенциально удовлетворяющих решению поставленных задач, что обеспечивает возможность индивидуального подхода.

В работе предложен и обоснован способ определения текущего уровня защищенности системы по ее профилю зрелости безопасности, установления приоритета практик безопасности друг перед другом, а также компенсации одних практик другими, заключающийся в использовании адаптированного метода анализа иерархий в качестве системы поддержки принятия решений эксперта.

Рыбаков С.Д. (автор) Подпись

Рудина Е.А. (научный руководитель) Подпись