МОДЕЛЬ БЕЗОПАСНОСТИ В НЕФТЕГАЗОВОЙ ОТРАСЛИ

Евгений ПИТОЛИН,
управляющий директор
Kaspersky
в Казахстане, Центральной Азии и Монголии

050010, Республика Казахстан,
г. Алматы, Казыбек би, 20а (Медеуский район)

Разработка стратегии защиты от киберугроз для нефтегаза – непростая задача, особенно для его промышленных систем и интернета вещей. В процессах проектирования, разработки, интеграции, использования и сопровождения таких систем принимает участие большое количество сторон.

Оценка рисков, связанных с атаками, у разных участников отличается, при этом безопасность для бизнеса определенных игроков может быть как отрицательным стимулом (увеличение времени выхода на рынок для продукта из-за необходимости реализовать требования безопасности), так и положительным (безопасный продукт – это еще и конкурентное преимущество с точки зрения маркетинга).

ПОЧЕМУ И ЗАЧЕМ НУЖНА МОДЕЛЬ ЗРЕЛОСТИ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Так, производители продуктов для автоматизации технологического процесса до сих пор пытаются переложить ответственность за обеспечение безопасности своих продуктов на клиентов, утверждая, что их продукт должен быть использован в изолированной (от интернета, от офисной сети и т. д.) среде. При этом они упорно игнорируют объективную реальность, в которой большинство предприятий в погоне за увеличением эффективности своей работы оказываются не в состоянии эти требования выполнить.

С другой стороны, мы нередко слышим от представителей предприятий различных отраслей, что они не могут (или не хотят) применить те или иные меры (установить патч ОС, например) и средства безопасности (установить антивирус) к своим системам промышленной автоматизации (например, рабочему месту оператора) без подтверждения со стороны производителя продукта.

Поиск баланса бизнес-стимулов в случае безопасности приводит к стратегии «балансирования на грани». Чтобы удержать равновесие, каждая из сторон – производители определенных видов оборудования, программного обеспечения, системные интеграторы, поставщики услуг, посредники, владельцы предприятий – ищут оптимальный набор мер безопасности и пытаются не выйти за рамки бюджета.

«ДОСТАТОЧНАЯ БЕЗОПАСНОСТЬ»

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.

В некоторых случаях кибератаки могут представлять существенную угрозу для организаций, даже если их прямой вины в инциденте нет. Например, для предприятия, отнесенного к КВОИКИ, аварийные ситуации, вызванные кибератакой, недопустимы, даже если они обусловлены эксплуатацией незакрытых производителем уязвимостей.

ЦЕЛЬ МОДЕЛИ ЗРЕЛОСТИ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Правильный выбор мер и средств обеспечения безопасности не всегда очевиден. Более того, локальные бизнес-цели и мотивированные ими решения по безопасности, принимаемые различными участниками процесса обеспечения безопасности (например, производителем и потребителем ОТ-продуктов и услуг) могут оказаться не только разными, но и несовместимыми.

Конечная цель модели зрелости безопасности интернета вещей нефтегазовой отрасли – обеспечить соответствие способов защиты от киберугроз реальным бизнес-потребностям. Задача – сформировать конкретное описание состояния «достаточной безопасности» для системы, помочь ответственным за безопасность этой системы лицам в нефтянке, сфокусироваться на наилучших способах достижения этого состояния и определить соответствующие меры защиты.

Зрелая с точки зрения безопасности система характеризуется достаточным набором мер защиты, которые не влияют негативно на ее функциональность. При этом определения «достаточности защиты» и понятия «негативно влиять на функциональность» для каждой системы свои.

На уровне бизнес-стейк холдеров формируется запрос на «защиту оборудования от хакерских атак». Основная проблема в том, что представители бизнеса почти всегда не являются специалистами в области информационной безопасности. Уязвимость оборудования к атакам может быть, к примеру, обусловлена неудачной архитектурой ПО. В долгосрочной перспективе может рассматриваться дорогостоящий перевод оборудования на альтернативную, более устойчивую к атакам, платформу. Текущие

версии также требуют технической поддержки и сопровождения, включая проверку на наличие уязвимостей и выпуск обновлений безопасности. Обратная связь с потребителем продуктов для получения информации об уязвимостях и инцидентах также требует содержания специализированного сервиса.

Для решения задачи выбора необходимых мер и средств защиты бизнесу требуется системный подход, который связывает приоритеты с целями безопасности и меры безопасности – непосредственно с ожидаемым эффектом. Поскольку способов сделать систему более безопасной (или компенсировать в достаточной степени ее небезопасность) довольно много, требуется эти способы упорядочить, чтобы можно было сделать выбор в пользу наиболее подходящих вариантов.

РОЛЬ АРХИТЕКТУРЫ ВЫБОРА

С учетом различий в бизнес-потребностях и в условиях недостаточной информации о возможных кибератаках и неясного влияния этих атак на функционирование системы, вендор и клиент (а также другие заинтересованные организации и лица, например, регуляторы) могут считать разные сценарии атак более вероятными и потенциально опасными, и различные практики защиты – более приоритетными для реализации.

Оценка рисков, связанных с атаками, разнится на стороне вендора и клиента. Согласование приоритетов вендора и клиента, выбор мер защиты, полноты реализации этих мер и сроков реализации требует структурированного представления вариантов с возможностью хотя бы приблизительной оценки соотношения их эффективности и требуемых ресурсов, то есть архитектуры выбора.

Архитектура выбора – это систематизация вариантов, которая подталкивает людей к выбору способа действий и к началу этих действий, то есть в нашем случае – к созданию более безопасной системы.

КАК РАБОТАЕТ МОДЕЛЬ ЗРЕЛОСТИ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Иерархия практик обеспечения безопасности

Архитектурой выбора и ядром модели зрелости безопасности интернета вещей является иерархия практик обеспечения безопасности (securitypractices). 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. Чтобы максимально упростить процесс выбора, на самом верхнем уровне группы практик объединяются в домены.

Три верхнеуровневых домена безопасности включают:

- управление безопасностью и организационные меры (Governance),
- обеспечение безопасности в силу конструкции (bydesign, Enablement)
- укрепление безопасности (Hardening).
- Приоритет того или иного домена перед другим для вендора определяется потребностями бизнеса и особенностями системы.