Kaspersky ICS CERT

kaspersky

Оценка зрелости кибербезопасности продукта

Проблема

Сложности с формализацией оценки уровня защищенности решений и ее демонстрацией в качестве конкурентного преимущества, с которыми сталкиваются производители подобных продуктов.

Решение

Достоверная оценка зрелости безопасности продукта, которая включает анализ механизмов безопасности и мер защиты на всех этапах его жизненного цикла, служит подтверждением защищенности решения и дает потребителям уверенность в его устойчивости к киберугрозам.

Для кого

Производители умных и подключенных устройств специального назначения — сетевого оборудования, систем промышленного интернета вещей, транспорта, логистики, энергетики, сельского хозяйства, автоматизации зданий и технологического процесса.

Производители продуктов интернета вещей, с заданным набором функциональности — умные камеры, носимые персональные устройства (часы браслеты и проч.) умные детские игрушки и помощники, системы дополненной реальности, умные кормушки для животных.

Производители чипов — модемов, SoCов и проч.

Производители специализированных технологических решений, таких как менеджеры лицензий, среды выполнения программ PLC, системы OTA обновлений для интернета вещей, облачные платформы и т. п.

Проблематика

Зрелая с точки зрения безопасности система характеризуется достаточным набором мер защиты, которые не оказывают негативного влияния на ее функциональность. При этом понятия «достаточности защиты» и «негативного влияния на функциональность» для каждой системы свои. Не всем продуктам и решениям подходят один и тот же уровень защиты и одинаковые процедуры обеспечения их кибербезопасности. Каждый производитель самостоятельно определяет приоритеты в вопросах

кибербезопасности, необходимые и достаточные для защиты решения. Зрелость в большей степени определяется не наличием множества разных механизмов, а тем, насколько целесообразно и эффективно они применяются.

Для выбора необходимых мер и средств защиты бизнесу нужен системный подход, который связывает приоритеты с целями безопасности, а меры — с ожидаемым эффектом. Поскольку может существовать не один способ сделать систему чуть более безопасной, надо описать, упорядочить и сделать понятными критерии выбора наиболее подходящих вариантов.

Чтобы продемонстрировать потребителю, что продукт надежно защищен, нужно предоставить ему информацию о целях, приоритетах обеспечения безопасности для продукта и действующих ограничениях (например, безопасность не может быть обеспечена за счет нарушения выполнения операций в реальном времени, если такое выполнение требуется при использовании продукта). Эта информация содержится в так называемом профиле зрелости безопасности продукта. Профиль используется совместно со свидетельством о зрелости безопасности, чтобы конкретизировать, чего именно потребителю стоит ждать от продукта по части обеспечения мер и механизмов защиты от кибератак.

Может показаться, что ограничения нельзя рассматривать как конкурентное преимущество продукта или решения, однако на деле четко описанная ответственность и оговоренные условия позволяют предотвратить избыточные ожидания от продукта/решения и продемонстрировать его действительно сильные стороны.

О Модели зрелости безопасности интернета вещей

Свидетельство о зрелости безопасности — своего рода знак отличия, который помогает вендору продвигать свой продукт или технологическое решение, а для потребителя означает определенную уверенность в этом продукте или решении. Свидетельство выдается после подтверждения соответствия способов защиты от киберугроз бизнес-потребностям, которое регламентирует Модель зрелости безопасности интернета вещей (IoT Security Maturity Model). В 2019 году Консорциум промышленного интернета вещей выпустил практическое руководство по применению этой модели.

> Опираясь на требования модели, мы подробно описываем состояние достаточной безопасности для конкретной системы и помогаем ответственным лицам определить наиболее эффективные способы достижения этого состояния и соответствующие меры защиты.

Использование модели зрелости позволяет вендору:

- оптимизировать постановку задачи безопасности, то есть определить уровень достаточной безопасности и описать все разумные ограничения;
- провести оценку и детальное планирование объема работ, необходимых для достижения достаточной безопасности;
- провести на техническом уровне оценку соответствия текущего состояния профилю зрелости безопасности, установленному на основе бизнес-требований, и при соответствии — получить подтверждающее свидетельство, заверенное «Лабораторией Касперского».

Что мы предлагаем

Сервис оценки зрелости безопасности продукта или технологического решения

Мы предлагаем сервис зрелости безопасности продукта или технологического решения, включающий профилирование и комплексную оценку этого продукта или решения в соответствии с особенностями их применения, позицией на рынке и отраслевой спецификой.

Профилирование предусматривает описание индивидуального профиля зрелости безопасности, который содержит необходимые и достаточные требования к организации и реализации практических мер безопасности и указывает на ограничения этих мер. Такие меры называются практиками безопасности.

Оценка практик безопасности учитывает технические и организационные аспекты обеспечения безопасности, а также их реализацию. Процесс оценки обязательно включает поиск уязвимостей в текущей версии продукта или решения, но не ограничивается им.

Результатом является получение производителем свидетельства о соответствии реализации практик безопасности профилю зрелости безопасности для продукта или решения.

Преимущества

- Оценка происходит не по обобщенным критериям кибербезопасности, разработанным для многих продуктов, а по индивидуально разработанному профилю безопасности.

- Методика профилирования и оценки основана на признанном международном стандарте Модели зрелости безопасности интернета вещей, разработанном Консорциумом промышленного интернета вещей при нашем активным участии.
- Учитываются ограничения на реализацию практик безопасности, обусловленные требованиями отрасли или особенностями применения продукта, что позволяет предусмотреть компенсирующие меры.
- Направленный поиск и оценка обнаруженных уязвимостей составляют часть процедуры оценки продукта, ее результаты используются в комплексе критериев оценки зрелости безопасности.

Как мы работаем

В сотрудничестве с заказчиком мы определяем цели безопасности продукта, подлежащего оценке, рассматриваем контекст применения продукта и другие необходимые условия. Затем мы сопоставляем эти цели и задачи, которые должны быть решены для уменьшения рисков безопасности. Всего рассматривается три класса, или домена, таких задач: управление вопросами безопасности продукта на протяжении его жизненного цикла, внедрение механизмов защиты и поддержание безопасности продукта при его эксплуатации.

На основе данных, предоставленных заказчиком, мы описываем:

- приоритетность решения задач обеспечения безопасности;
- степень необходимой полноты решения каждой задачи;
- объективно существующие ограничения.

Таким образом мы создаем индивидуальный профиль подлежащего оценке конечного продукта или технологического решения с точки зрения требований безопасности.

Профиль зрелости безопасности определяет, что именно нужно сделать в отношении организационных мер безопасности и технических механизмов защиты от атак, чтобы цели безопасности были достигнуты.

При помощи профиля мы определяем, какие задачи нужно решить техническому персоналу заказчика для достижения целевого уровня зрелости безопасности с учетом особенностей отрасли и продукта.

После этого на основе профиля зрелости безопасности исследуем продукт и процессы заказчика, чтобы установить соответствие требованиям профиля. Мы привлекаем различных специалистов и представителей

различных департаментов со стороны заказчика, чтобы получить необходимые сведения о процессах разработки, выпуска и сопровождения. Исследование продукта включает анализ его архитектуры, функций безопасности, поиск и анализ уязвимостей.

Если какой-либо процесс или механизм не соответствует профилю, мы выдаем заказчику рекомендации по устранению этого несоответствия. После устранения проводим повторную оценку проблемного процесса или механизма.

В некоторых случаях мы модифицируем профиль зрелости безопасности, если обнаруживаем критические несоответствия, которые не могут быть устранены по объективным причинам, не идентифицированным на момент разработки профиля.

Создание профиля зрелости безопасности продукта позволяет предоставить потребителю объективную информацию о продукте и его гарантиях безопасности в форме свидетельства, содержащего ссылку на профиль.

Результат

Заказчик получает свидетельство о зрелости безопасности, содержащее ссылку на профиль зрелости безопасности. Это свидетельство может быть использовано как объективное подтверждение реализации мер и механизмов безопасности для продукта или технологического решения и способствовать продвижению продукта или решения на рынке.

Помимо этого, заказчик получает:

- полный отчет об обследовании продукта и процессов, связанных с его разработкой, выпуском и сопровождением;
- отчет об оценке уязвимостей в текущей версии продукта;
- перечень рекомендаций по улучшению продукта и процессов, который может быть использован также и для схожих продуктов и решений.

Отличие от сервиса оценки уязвимостей

Сервис по оценке уязвимостей не позволяет однозначно подтвердить безопасность продукта или решения, поскольку ни одна методика обследования не дает возможности выявить все уязвимости, можно говорить только о том, были уязвимости обнаружены на момент оценки или нет.

Сервис оценки зрелости безопасности позволяет не только обнаружить уязвимости и предложить рекомендации по их устранению, но еще и подтвердить, что заказчик реализовал необходимые меры для предотвращения эксплуатации уязвимостей продукта и их своевременного устранения в случае их обнаружения в будущем.

Помимо этого, оценка зрелости безопасности продукта:

- учитывает контекст применения устройства, ограничения отрасли, в которой оно применяется, требования к другим аспектам безопасности и функционирования устройства;
- может применяться не только к текущей версии этого продукта, но и к его будущим версиям в случае должного поддержания процессов сопровождения;
- позволяет реализовать другие продукты с учетом полученной оценки зрелости безопасности продукта и рекомендаций по улучшению продукта и процессов.

В отличие от стандартов и базовых рекомендаций регуляторов по улучшению безопасности, руководство по улучшению продукта и процессов на основе профиля зрелости исключает формальный подход и рекомендует только те механизмы обеспечения безопасности, которые соответствуют условиям и сценариям использования этих устройств.

Сценарии использования

Оценка зрелости безопасности готового продукта, присутствующего на рынке

Заказчик может предоставить уже выведенный на рынок продукт для оценки его зрелости безопасности. Это самый простой вариант, поскольку отсутствует какая-либо неопределенность в аспектах реализации и сопровождения продукта: мы строим профиль зрелости безопасности согласно приоритетам заказчика, а затем оцениваем то, что видим, и сравниваем.

При соответствии технических и организационных мер безопасности профилю зрелости безопасности, учитывающему ограничения и особенности обеспечения безопасности для отрасли и конкретного устройства, мы выдаем свидетельство о зрелости безопасности продукта. Свидетельство содержит отсылку к описанию профиля зрелости безопасности и должно рассматриваться только совместно с этим профилем.

Однако единственным способом устранения некоторого несоответствия профиля зрелости с реальным положением вещей для готового продукта может быть снижение уровня зрелости, гарантируемого профилем. Заказчик при этом получает рекомендации для исправления архитектурных недостатков функций безопасности, которые он сможет учесть при разработке новой версии продукта.

Оценка зрелости безопасности нескольких продуктов или линейки продуктов, присутствующих на рынке

Более сложным, но экономически эффективным вариантом является оценка зрелости безопасности нескольких однотипных продуктов или линейки продуктов. Для них разрабатывается единый профиль зрелости безопасности, а затем оценивается каждый продукт или характеристические (обычно наиболее полнофункциональные) представители линейки продуктов, выбранные совместно с заказчиком. В последнем случае мы обязательно подключаем технических экспертов, выполняющих анализ использования единого программного кода и требований к аппаратной платформе в каждом решении, подлежащем оценке.

При соответствии технических и организационных мер безопасности профилю зрелости безопасности, учитывающему ограничения и особенности обеспечения безопасности для отрасли и рассматриваемых устройств, мы выдаем свидетельство о зрелости безопасности продуктов или линейки продуктов. Свидетельство содержит перечень продуктов и все признаки для их идентификации, отсылку к описанию профиля зрелости безопасности для этих продуктов и должно рассматриваться только совместно с этим профилем.

Так же, как и в предыдущем сценарии, при обнаружении несоответствия мы предлагаем снизить уровень зрелости, гарантируемый профилем, и доработать продукт с учетом выявленных недостатков.

Подготовка профиля зрелости безопасности, разработка продукта по требованиям профиля и засвидетельствование результата

Если необходимо, чтобы оцениваемый продукт в точности соответствовал ожиданиям бизнеса, то оптимальным вариантом будет начать с разработки профиля зрелости безопасности согласно этим ожиданиям, и затем

перевести его требования в техническую плоскость, чтобы реализовать их в продукте и поддерживающих его процессах.

Чем раньше начинается работа по формированию требований профиля зрелости безопасности, тем легче впоследствии обеспечить выполнение этих требований в продукте. Важную роль в оценке играют процессы разработки продукта: их зрелость, четко определенные критерии безопасности при работе с кодом сторонних производителей и открытым кодом, процедуры установления требований и тестирования безопасности. Процессы не могут быть изменены за один день, если это потребуется.

Тем не менее подготовка профиля и проведение оценки зрелости безопасности возможны на любом этапе до запуска продукта в эксплуатацию.

В этом сценарии работы мы также строим профиль согласно ожиданиям заказчика, затем оцениваем имеющиеся технические требования, процессы и решения в рамках разработки продукта. Результат представляем в виде описания текущего состояния зрелости продукта и вырабатываем рекомендации по улучшению процессов и решений так, чтобы итоговый продукт соответствовал профилю зрелости безопасности. Рекомендации представляем в виде дорожной карты по улучшению зрелости безопасности продукта до его выпуска и запуска в эксплуатацию.

Важно понимать, что в процессе разработки продукта бизнес-видение может меняться, поэтому мы можем периодически пересматривать целевой профиль зрелости безопасности, рекомендации и дорожную карту. Мы участвуем в процессе разработки и проводим периодические согласованные проверки зрелости безопасности вплоть до выпуска продукта. Также мы сопровождаем разработку продукта на этапе тестирования и интеграции, в том числе выполняя оценку уязвимостей, чтобы уязвимости могли быть устранены до выпуска продукта.

Этот процесс завершается выпуском продукта, признанного соответствующим целевому профилю зрелости безопасности. По запросу заказчика этот процесс реализуется для группы или линейки продуктов.

Запросить консультацию специалиста

Статьи по теме

- Модель зрелости безопасности интернета вещей: толчок к развитию безопасных систем

- Security Maturity Model: Practitioner's Guide. Описание Модели зрелости безопасности Консорциума промышленного интернета вещей
- Исследование безопасности модема Cinterion EHS5 3G UMTS/HSPA
- Секреты протокола Schneider Electric UMAS
- Динамический анализ компонентов прошивок IoT-устройств
- ISaPWN — исследование безопасности ISaGRAF Runtime
- Практический пример фаззинга приложений OPC UA
- Исследование уязвимостей в VNC
- Исследование безопасности: CODESYS Runtime — фреймворк для управления ПЛК. Часть 1
- Исследование безопасности: CODESYS Runtime — фреймворк для управления ПЛК. Часть 2
- Исследование безопасности: CODESYS Runtime — фреймворк для управления ПЛК. Часть 3
- Как мы взломали умный дом нашего коллеги, или утренний Drum & Bass
- Исследование безопасности: ThingsPro Suite — IIoT-шлюз и менеджер устройств от компании Moxa
- Исследование безопасности OPC UA
- Больше, чем «умные» камеры. Под присмотром неустановленных лиц
- Серебряная пуля для атакующего. Исследование безопасности лицензионных токенов

Рекомендуем дополнительно

- Поток машиночитаемых данных об уязвимостях АСУ ТП
- Расследование киберинцидентов на промышленных предприятиях
- Информация об уязвимостях и угрозах для АСУ ТП

Запросить консультацию специалиста

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com