IEC 62443 КАК ГАРАНТИЯ БЕЗОПАСНОСТИ РЕШЕНИЙ ZENON

COPA-DATA и TÜV SÜD плодотворно сотрудничают на протяжени долгого времени. В этой статье мы рассмотрим, какие части данного стандарта применимы к независимому поставщику программного обеспечения, такому как COPA-DATA, и почему сертификация имеет смысл.

Для поставщиков, таких как COPA-DATA, в общем случае имеют значение следующие части стандарта:

- **IEC 62443 3.1** – Технологии безопасности для промышленной автоматизации и систем управления
- **IEC 62443 3.3** – Требования к безопасности системы и уровни безопасности
- **IEC 62443 4.1** – Требования к жизненному циклу безопасной разработки продукта

В отличие от первых двух частей, рассматривающих более технический подход к данной теме, часть 4.1 посвящена основным положениям, таким как процессы планирования и разработки и мероприятия по обеспечению качества (QA). В COPA-DATA большее внимание уделяется части 4.1, поскольку любая будущая разработка продукта или функции будет основываться на внедренной оптимизации процессов и политик.

СТАНДАРТНЫЕ И ОПРЕДЕЛЯЕМЫЕ ПРОЦЕССЫ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ РАЗРАБОТКИ ПРОДУКТА

По существу, стандарт IEC 62443 4.1 определяет процедурные требования для безопасной разработки продуктов, используемых в системах промышленной автоматизации и управления. Он определяет требования к жизненному циклу безопасной разработки (SDL), которые должны применяться к любому продукту в среде промышленной автоматизации и управления.

Описание жизненного цикла включает в себя:

- определение требований безопасности
- безопасное проектирование
- безопасное внедрение (вкл. руководство по кодированию)
- проверку и валидацию
- управление ошибками
- управление исправлениями
- управление информацией, касающейся безопасности.

Эти требования можно применять к существующим процессам разработки, поддержки и окончанию жизни программного обеспечения, такого как zenon. Текущая версия этой части была выпущена 15 января 2018 года и не планируется к пересмотру вплоть до 2022 года.

КАК IEC 62443 4.1 ГАРАНТИРУЕТ БЕЗОПАСНУЮ И ВЫСОКОКАЧЕСТВЕННУЮ РАЗРАБОТКУ ZENON

Давайте посмотрим, что же произошло в COPA-DATA, и как мы адаптировались, чтобы соответствовать требованиям стандарта TÜV SÜD, и как это в конечном итоге отразилось на вас, пользователях zenon.

Прежде всего, в COPA-DATA был создан Отдел Управления Безопасностью (SMT), который согласно стандарту должен работать в течение всего жизненного цикла разработки или, в контексте COPA-DATA, в течение одного релиза zenon.

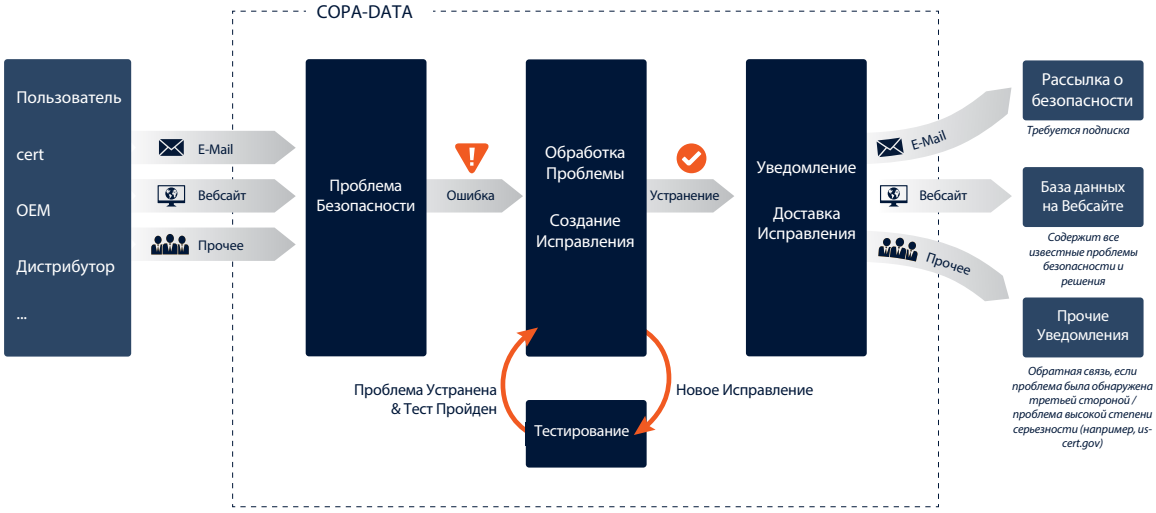

Рисунок 1:
Менеджмент проблем безопасности в COPA-DATA

Основной задачей отдела является планирование, мониторинг и информирование о повышении безопасности продуктов и сервисов COPA-DATA, а также мониторинг и информирование о возможных проблемах безопасности, связанных со встроенными компонентами сторонних производителей. В случае обнаружения каких-либо уязвимостей, связанных с этими компонентами, COPA-DATA проинформирует своих клиентов о возникшей проблеме.

На протяжении всего жизненного цикла другой важной обязанностью отдела является мониторинг и оценка процессов, внедренных в COPA-DATA и связанных с безопасностью. В этой связи, он играет очень важную роль в управлении качеством с точки зрения непрерывного процесса оптимизации.

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ И ОПРЕДЕЛЕНИЕ ПРИОРИТЕТА ПРОБЛЕМ

Еще одним важным нововведением стало внедрение моделей угроз и приоритизация вопросов безопасности на основе общей системы оценки уязвимостей (CVSS). Процесс использования моделей угроз является эффективным способом управления потенциальными угрозами для таких сложных систем, как zenon. Отдел Управления Безопасностью использует этот метод для поиска структурных уязвимостей с точки зрения потенциального злоумышленника. Эта модель помогает нам, как "защитнику", проводить систематический анализ потенциальных векторов атак, а также получить четкое представление об активах, наиболее привлекательных для атакующего. Эти модели угроз дают нам ответы на самые важные вопросы в контексте безопасности: "Где мои ценные активы?", "Где моя самая большая уязвимость?" и "Какие самые актуальные угрозы?".

На основе этих моделей Отдел Управления Безопасностью получает более четкое представление о том, где необходима оптимизация продукта - в плане функций или структуры.

Следующий шаг - это использование общей системы оценки уязвимостей для ранжирования выявленных угроз, которое позволит определить степень серьезности выявленных уязвимостей в системе безопасности. Таким образом, данный открытый отраслевой стандарт позволяет четко определить приоритетность выявленных угроз. Помимо того, что это отличный способ приоритизации проблем, использование такой оценки является хорошим способом получить четкое представление о ресурсах, необходимых для устранения угрозы.

Баллы рассчитываются с помощью стандартизированных инструментов, отражающих простоту использования уязвимости и эффект от ее использования. Баллы варьируются от 0 до 10, причем 10 - самые сильные (типичный пример https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator). В COPA-DATA все зарегистрированные ошибки безопасности и запросы

COPA-DATA сертифицирована по стандарту безопасности ISA/IEC 62443-4-1:2018.
На фото: Марк Клеменс (слева) и Рейнхард Майр (справа) с сертификатом TÜV SÜD.

новых функций оцениваются на основе этой системы подсчета очков.

ТЩАТЕЛЬНОЕ ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ, А ТАКЖЕ УЛУЧШЕНИЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ КАЧЕСТВА И ОБСЛУЖИВАНИЯ КЛИЕНТОВ

Улучшенные стратегии обеспечения качества также рассматривались в рамках реализации процесса обеспечения безопасности в COPA-DATA. Вдобавок к нашим существующим мероприятиям в области обеспечения качества, мы ввели также внутренние тесты на проникновение, которые проводятся для каждого релиза zenon. Мы используем два различных метода проведения теста на проникновение: слепое тестирование и внутреннее тестирование на проникновение.

Метод **слепого тестирования** имитирует действия и процедуры реального злоумышленника, существенно ограничив исходную информацию, предоставляемую человеку или команде, выполняющей тест. Как правило, им может быть дано только название компании. Поскольку этот тип испытаний может потребовать значительного количества времени для разведки, он может оказаться весьма дорогостоящим.
Также мы ввели **внутреннее тестирование на проникновение**: тест, который имитирует внутреннюю атаку за брандмауэром, авторизованным пользователем со стандартными правами доступа. Такой тест полезен. например, для оценки того масштаба ущерба, который способен нанести недовольный сотрудник.

В настоящее время COPA-DATA находится на первом году внедрения всех этих новых стандартов, процедур и инструментов. Мы уже видим положительное влияние на наши продукты и процессы. Благодаря этому и формализации стандарта, наши клиенты знают, что они могут положиться на нашу профессиональную обработку всех проблем безопасности - не только в рамках продукта и его функций, но и, конечно, с точки зрения профессионального общения и управления проблемами.

РЕЙНХАРД МАЙР,
НАЧАЛЬНИК ОТДЕЛА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
И НАУЧНЫХ ИССЛЕДОВАНИЙ