ПЕРВЫЙ В МИРЕ ПРАКТИЧЕСКИЙ ОПЫТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ: «БОМБАРДЬЕ ТРАНСПОРТЕЙШН (СИГНАЛ)» ВНЕДРЯЕТ PT ISIM НА ДОРОГАХ ОАО «РЖД»

ЗАДАЧА

ООО «Бомбардье Транспортейшн (Сигнал)» — первое международное совместное предприятие на сети российских железных дорог, созданное ОАО «РЖД» и компанией Bombardier Transportation, крупнейшим в мире производителем железнодорожной техники.

Основной задачей «Бомбардье Транспортейшн (Сигнал)» является внедрение передовых систем управления движением поездов на российском рынке. В своих решениях компания активно использует систему микропроцессорной централизации (МПЦ) EBILock 950, которой уже оснащено свыше 170 зарубежных станций и более 180 станций на 15 железных дорогах по всей России. Гибкость и устойчивость МПЦ EBILock 950 позволяют использовать ее в решениях для магистральных железных дорог, а также на высокоскоростных железнодорожных линиях и метрополитенах.

Активный рост технологичности российских железнодорожных станций привел к тому, что функциональная безопасность систем управления движением поездов оказалась напрямую зависимой от растущего уровня киберугроз в транспортной отрасли. Это потребовало от «Бомбардье Транспортейшн (Сигнал)» активных действий по повышению защищенности объектов, оснащенных МПЦ EBILock 950.

РЕШЕНИЕ

В качестве решения для защиты железнодорожных станций была выбрана система управления инцидентами информационной безопасности АСУ ТП, разработанная компанией Positive Technologies, — PT Industrial Security Incident Manager (PT ISIM).

PT ISIM предназначен для эффективного обнаружения и предотвращения кибератак, направленных на АСУ ТП. Не оказывая влияния на работу промышленной системы, PT ISIM обеспечивает постоянный мониторинг сетевой активности, выявляет события информационной безопасности и связи между ними. При этом уникальные возможности визуализации инцидентов в PT ISIM помогают оперативно определять векторы распределенных во времени атак и соотносить их с элементами технологического процесса промышленного объекта, в том числе такого, как железнодорожная станция.

PT ISIM выполняет сбор и обработку данных исключительно в пассивном режиме. Эта ключевая особенность решения обеспечила введение PT ISIM в пилотную, а затем и в промышленную эксплуатацию без приостановки технологического процесса и нарушения работы железнодорожных узлов. Промышленное исполнение серверного оборудования PT ISIM подходит для работы в системах управления ответственными процессами, где безопасность и надежность функционирования системы выходят на первый план.

Ролевая модель управления доступом, примененная в PT ISIM, позволила создать для заказчика удобную среду реагирования на нарушения кибербезопасности. В случае возникновения инцидента PT ISIM предоставляет ответственным сотрудникам предприятия информацию, соответствующую их полномочиям. Оперативный персонал располагает минимальным набором инструментов, необходимых для поддержки административных регламентов, а сотрудники службы ИБ получают полный доступ к информации об инцидентах для их расследования.

В рамках сервиса оценки уровня защищенности АСУ ТП эксперты компании Positive Technologies также провели комплексный аудит безопасности информационной системы железнодорожной станции, оснащенной МПЦ EBILock 950. Результаты аудита позволили не только сформировать актуальную модель угроз и детально проработать требования к системе защиты, но и оперативно устранить обнаруженные уязвимости. Там, где устранение уязвимостей было затруднено из-за архитектурных особенностей системы, были реализованы необходимые компенсационные меры, предложенные экспертной командой Positive Technologies и головной организацией по кибербезопасности ОАО «РЖД».

ПРОФИЛЬ ОРГАНИЗАЦИИ

- **Название:** ООО «Бомбардье Транспортейшн (Сигнал)»
- **Отрасль:** железнодорожный транспорт
- **Задача:** повысить защищенность станций, оснащенных передовыми системами управления движением поездов (МПЦ EBILock 950)
- **Решение:** система управления инцидентами кибербезопасности PT Industrial Security Incident Manager (PT ISIM)

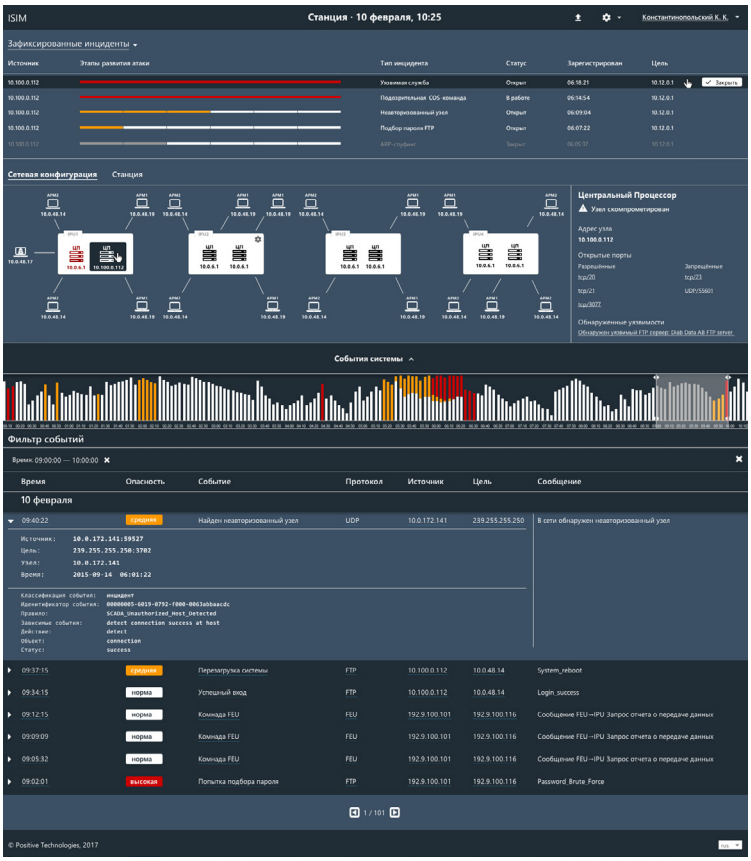
«Лучшее отраслевое решение» Global CIO 2016

«Это первый практический опыт в мире обеспечения киберзащищенности микропроцессорных систем управления движения поездов. Мы благодарны компании «РЖД» за инициацию этого проекта и помощь в его осуществлении. Полученные результаты могут быть интересны для использования за рубежом».

В. А. Гросс,
первый заместитель генерального директора ООО «Бомбардье Транспортейшн (Сигнал)»

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Сбор данных без вмешательства в технологический процесс
- Поддержка промышленного оборудования и протоколов связи
- Обработка событий с учетом элементов и логики техпроцесса
- Визуализация инцидентов на технологических схемах
- Анализ и визуализация развития атак в виде цепочек событий
- Расследование инцидентов без остановки АСУ ТП
- Информирование об инцидентах на всех уровнях ответственности



РЕЗУЛЬТАТЫ

Проведенные в рамках проекта работы позволили компании «Бомбардье Транспортейшн (Сигнал)» значительно повысить уровень защищенности системы МПЦ EBILock 950. Вслед за развертыванием на опытной железнодорожной станции, оборудованной МПЦ EBILock 950, PT ISIM успешно прошел заводские испытания и был принят в постоянную эксплуатацию.

«Это значимый проект для нашей компании и для отрасли в целом. Совместный с Positive Technologies проект стал практическим воплощением нашего подхода к кибербезопасности, суть которого в переходе от вопроса поиска уязвимости к конкретным решениям», — отмечает первый заместитель генерального директора ООО «Бомбардье Транспортейшн (Сигнал)» Вадим Гросс.

По итогам 2016 года крупнейшее российское сообщество IT-директоров Global CIO признало проект внедрения PT ISIM на дорогах ОАО «РЖД» победителем в номинации «Лучшее отраслевое решение» категории «Транспорт и логистика». Ранее проект и решение на базе PT ISIM были отмечены экспертным советом по кибербезопасности ОАО «РЖД» и завоевали первое место в номинации «Системы диагностики и управления» в конкурсе ОАО «РЖД» на лучшее качество подвижного состава и сложных технических систем.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

ptsecurity.ru
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays