alperia

2020

Обеспечение безопасной и бесперебойной работы электросетей

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Industrial CyberSecurity

Компания Alperia выбрала Kaspersky Industrial CyberSecurity for Nodes для защиты своих систем удаленного управления. Эти системы обслуживают электростанции и распределительную сеть, поставляющие электроэнергию 280 000 клиентам в Южном Тироле. Компания нуждалась в специализированном решении для максимальной защиты промышленной среды без риска перебоев в работе критически важного оборудования.

Рост числа подключенных устройств и цифровая трансформация инфраструктуры коммунальных предприятий открывают новые возможности. Но вместе с тем возрастают и риски.

Согласно глобальному отчету о рисках за 2020 г., подготовленному Всемирным экономическим форумом, масштабные кибератаки и возможные перебои в работе критически важных инфраструктур и информационных сетей находятся на втором месте среди самых опасных рисков.

Также, согласно прогнозу рисков Allianz Risk Barometer на 2020 г., киберинциденты занимают первое место среди корпоративных рисков (в глобальном масштабе); на втором месте риски, связанные с перебоями в бизнесе.

Неудивительно, что компании, предоставляющие жизненно важные услуги (водо- и электроснабжение, транспорт, телекоммуникации), уделяют все больше внимания защите своих инфраструктур. Это относится и к предприятиям, производящим и распределяющим электроэнергию.

«Мы организовали рабочую группу совместно с экспертами “Лаборатории Касперского”, что позволило адаптировать решение к специфике нашейкомпании».

Сандро Моретти (Sandro Moretti),
руководитель отдела телеуправления и телекоммуникаций компании Alperia

Электричество и газ для 280 000 жителей Южного Тироля

Alperia – компания в Южном Тироле (автономная провинция в Италии), осуществляющая электро- и газоснабжение для 280 000 клиентов. В ее ведении находятся 34 гидроэлектростанции, шесть районных теплоцентралей, более 8600 километров линий электропередач и 700 зарядных станций.

Компания была основана в 2016 г. посредством слияния двух ключевых местных энергетических компаний. Это AEW, чья история уходит в конец XIX века, когда ее предшественница Etschwerke построила первые гидроэлектростанции для электрификации области, и SEL – энергетическая компания Южного Тироля, в последнее десятилетие взявшая на себя управление крупными ГЭС и электросетью.

Отдел телеуправления и телекоммуникаций Alperia Group возглавляет инженер Сандро Моретти, подчиняющийся непосредственно генеральному директору группы компаний. Под его началом – отдел из 13 человек, которые контролируют передачу данных производственных систем и телекоммуникации. Отдел отвечает за работу удаленных конечных устройств (RTU), центров обработки данных, пунктов управления и сети, связывающей два основных подразделения группы. Первое (Alperia Greenpower) занимается генерацией электроэнергии, а второе (Edyna) – ее распределением.

Специфика промышленной среды

Моретти убежден, что защита промышленных систем с помощью традиционных решений – не самая удачная идея. Кибербезопасность данных предполагает их конфиденциальность, целостность и доступность – именно в таком порядке. Однако в случае операционных технологий (OT) порядок строго обратный. В особенности это относится к критически важным инфраструктурам, где системы должны работать бесперебойно (именно поэтому для управления ими используется оборудование с резервированием).

Следовательно, в промышленной сфере защитные решения должны проектироваться с учетом особенностей конкретных сред. Порты, протоколы и правила для устройств, подключенных к сети предприятия и системам удаленного управления, могут сильно различаться. Также следует учитывать, что установленные на оборудовании операционные системы должны работать бесперебойно, поэтому установка исправлений безопасности в режиме реального времени возможна далеко не всегда.

Около 990
сотрудников

1,3 млрд €
выручки

1 056 717 €
инвестировано в исследования

«С самого начала руководство компании понимало, что в защите OT нельзя руководствоваться принципами IT-безопасности, – говорит Моретти. – Именно поэтому Alperia отделила периметр OT-сети от IT-сети и разработала разные стратегии управления ими».

Затем группа под началом Моретти приступила к поиску решения, которое можно использовать внутри периметра. Но не традиционную защиту конечных устройств вроде той, что используется в IT-сфере, а более совершенную, учитывающую специфику OT-среды.

После тщательного анализа немногих доступных на рынке решений для защиты промышленных сред Моретти выбрал Kaspersky Industrial CyberSecurity.

Однако установка защитного решения для систем, работающих без перерывов, – непростая задача. Поэтому Alperia и «Лаборатория Касперского» создали совместную рабочую группу, чтобы обеспечить максимально эффективное развертывание решения.

Такое сотрудничество полностью себя оправдало – особенно учитывая, что в Alperia не было тестовой среды, то есть работать пришлось на реальном оборудовании.

Персонализированное внедрение

Мы приступили к внедрению в конце 2018 г., начав с проверки концепции: Kaspersky Industrial CyberSecurity for Nodes работало на выбранных машинах в течение нескольких недель.

«Нам было очень важно испытать решение в реальных условиях: оценить его влияние на работу машин, понять, какие нужно задать исключения и какие требуются оптимизации, – рассказывает Моретти. – В Alperia все системы работают с резервированием. Мы установили решение только на одну из двух машин (на основную), чтобы в случае проблем у нас была подстраховка и производство не пострадало. Так нам удалось провести различные стресс-тесты, и все они были успешно пройдены».

Изначально решение Kaspersky Industrial CyberSecurity было запущено в режиме мониторинга.

«Мы хотели проверить, будет ли новая система давать ложноположительные срабатывания и замедлять работающие приложения; есть ли риск блокирования тех или иных критически важных служб. Когда мы убедились, что система прекрасно справляется со своими задачами, мы задействовали все ее возможности, позволив Kaspersky Industrial CyberSecurity блокировать любые подозрительные службы, – поясняет Моретти. – На этом этапе наши инженеры обеспечили максимально подробную запись событий агента в журналы, чтобы проанализировать его взаимодействие с системой SCADA».

Защита промышленных данных
Защита предприятия для обеспечения непрерывности бизнеса

Контроль
Защита процессов мониторинга предприятия

Бесперебойная работа
Обеспечение предиктивного обслуживания

«После тщательного анализа журналов мы представили Alperia дополнительную информацию для конфигурации», – объясняет Диего Магни (Diego Magni), менеджер «Лаборатории Касперского» по предпродажной поддержке.

После окончания эксперимента рабочая группа постепенно внедрила систему на остальные машины и во все прочие среды (физические и виртуальные). «Сегодня около 40 наших серверов защищены решением «Лаборатории Касперского», – говорит Моретти. – Менее чем за полгода мы вышли на полную мощность и сделали это постепенно и совершенно безопасно».

Моретти доволен достигнутыми результатами и оказанной поддержкой. «Я убежден, что в случаях, подобных нашему, просто необходимо выходить за рамки традиционных отношений «клиент – поставщик» и переходить к более широкому партнерству. Поэтому сейчас мы обдумываем возможность заключения с «Лабораторией Касперского» договора о сервисном обслуживании. С ним мы получим не только техническую поддержку продукта, но и консалтинг по всему периметру сети», – подытоживает Моретти.

Больше о KICS: ics.kaspersky.ru

www.kaspersky.ru

kaspersky **АКТИВИРУЙ БУДУЩЕЕ**

© АО «Лаборатория Касперского», 2020. Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.