AGC

TOMORROW LABS

«Лаборатория Касперского» защищает завод AGC в Германии

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Industrial CyberSecurity

AGC Glass Germany

agc-automotive.com

tomorrow-connect.com

Производственный сектор

- Год основания: 2003
- Клиенты: BMW, Volkswagen, Mercedes, Volvo, Opel
- Использует решение Kaspersky Industrial CyberSecurity с 2016 года

AGC Glass Germany с 2003 года поставляет автомобильные стекла таким ведущим производителям, как BMW, Volkswagen, Mercedes-Benz, Volvo и Opel. На предприятии компании в Вегберге (рядом с Мёнхенгладбахом, Германия) работают 150 человек. AGC входит в состав японской группы Asahi Glass Company, крупнейшего в мире производителя стекла, который обеспечивает 54 000 рабочих мест в 30 странах мира.

AGC Glass Germany GmbH обрабатывает автомобильное стекло, изготовленное на других предприятиях группы, в соответствии с конкретными потребностями клиентов, например, устанавливает на стекло системы обогрева, датчики дождя или уплотнители. После этого компонент поступает на производство различных автомобилестроителей.

Особенности и приоритеты компании

«За 2 года использования Kaspersky Industrial CyberSecurity мы оценили индивидуальный подход „Лаборатории Касперского“ и динамичное развитие ее решения. В отношении сотрудничества этой компании также нет равных: мы всегда можем рассчитывать на эффективную командную работу и консультативную помощь».

Ян Хоубен, директор завода AGC Glass Germany GmbH

Для предприятий с крупносерийным стандартизированным производством, таких как AGC Glass Germany, стабильность процессов имеет критическое значение. В случае задержки производства или, еще хуже, полной остановки производственных линий клиенты могут потребовать не только возмещения за аннулирование заказа, но во многих случаях также уплаты значительных договорных неустоек. Для предотвращения таких ситуаций AGC использует платформу Tomorrow Connect, соответствующую стандартам индустрии 4.0, и инженерные приложения для нее (eApp). Это позволяет собирать информацию о стабильности процессов и отклонениях от заданных значений в режиме реального времени.

Решение было разработано партнером «Лаборатории Касперского» Tomorrow Labs в сотрудничестве с институтом Fraunhofer IPA и машиностроителями. Платформа собирает, связывает и визуализирует данные оборудования и ERP-систем на разных площадках предприятия, объединяя таким образом информацию из различных отделов в масштабе компании, что позволяет добиться прозрачности и автономности производства.

Объединение такого большого количества производственного оборудования в единую сеть приводит к возникновению новых уязвимостей. В случае атак возможны значительные финансовые и репутационные потери.

AGC осознает важность эффективного защитного решения. Его внедрение сулит множество выгод для бизнеса: снижение риска сбоев в производственных процессах, обеспечение безопасности цепочки поставок, соблюдение нормативных требований и т. д.

«Мы выбрали в качестве технологического партнера „Лабораторию Касперского“, поскольку это признанный поставщик защитных решений в сфере промышленной кибербезопасности. „Лаборатория Касперского“ располагает обширными экспертными знаниями и исследовательскими наработками и не только предоставляет программное обеспечение, но и осуществляет анализ угроз и оценку уязвимостей», – говорит Ян Хоубен, директор завода AGC Glass Germany GmbH.

Безопасность
Решение разработано специально для промышленных сред и сочетает мониторинг промышленных сетей с защитой рабочих мест

Управление рисками
Предотвращение ситуаций, в которых требуется уплата договорных неустоек из-за сбоев в поставках или недостаточного качества продукции

Целостность
Мониторинг целостности данных, передаваемых на панель управления оператора, позволяет защититься от самых изощренных атак

Интеграция с платформой Tomorrow Connect

Чтобы гарантировать безопасность, AGC выбрала решение Kaspersky Industrial CyberSecurity – специализированное решение для защиты промышленных систем управления.

Kaspersky Industrial CyberSecurity for Nodes защищает АСУ ТП, серверы SCADA, HMI и инженерные рабочие станции от различных киберугроз, которые могут быть связаны с человеческим фактором, вызваны обычными вредоносными программами, целевыми атаками или диверсиями. Kaspersky Industrial CyberSecurity for Networks работает на уровне промышленных протоколов связи (Modbus, IEC, ISO и т. п.), анализируя трафик на предмет аномалий с помощью технологии подробной проверки пакетов (DPI). Также этот компонент выполняет обнаружение устройств и визуализацию карты промышленной сети.

Через 2 года после первоначального внедрения Kaspersky Industrial CyberSecurity компания AGC решила расширить функциональные возможности проекта. AGC обновила установленные лицензии Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks до самых последних версий. Кроме того, «Лаборатория Касперского» обеспечила интеграцию Kaspersky Industrial CyberSecurity с платформой Tomorrow Connect, разработанной TomorrowLabs. Это открыло целый ряд новых полезных возможностей:

- телеметрические данные производства и статус киберзащиты отображаются на панели управления директора завода в режиме реального времени;
- Kaspersky Industrial CyberSecurity гарантирует, что данные телеметрии не будут скомпрометированы, и обеспечивает обнаружение аномалий и нарушений безопасности рабочих мест;
- Kaspersky Industrial CyberSecurity выявляет нарушения технологических процессов с помощью технологии DPI, что помогает избежать ошибок на производстве и гарантировать качество продукции.

Результаты

«Решение обеспечивает кибербезопасность на всех уровнях сети, не нарушая непрерывности наших технологических процессов».

Ян Хоубен, директор завода
AGC Glass Germany GmbH

«Лаборатория Касперского» вместе с TomorrowLabs успешно обновила продукты Kaspersky Industrial CyberSecurity и адаптировала их в соответствии с потребностями AGC. Этот проект обеспечил AGC полную защищенность и возможности оперативного реагирования, а также гарантии целостности при переносе данных в Tomorrow Connect. Теперь компания может быть уверена в своей безопасности и отсутствии сбоев в технологических процессах, равно как и в высоком уровне доверия со стороны партнеров по цепочке поставок.

«Решение Kaspersky Industrial CyberSecurity состоит из модулей, что позволяет адаптировать его к нашим специфичным потребностям и инфраструктурам, – добавляет Ян Хоубен. – Решение обеспечивает кибербезопасность на всех уровнях сети, не нарушая непрерывности наших технологических процессов».

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity — это набор технологий и сервисов, созданных для защиты различных уровней промышленной инфраструктуры и других элементов предприятия, в том числе серверов SCADA, операторских панелей, инженерных рабочих станций, ПЛК, сетевых соединений и даже самих инженеров. При этом решение не влияет на непрерывность технологических процессов.

Узнайте больше на: www.kaspersky.ru/ics

Kaspersky ICS CERT:
https://ics-cert.kaspersky.ru
Новости киберугроз:
www.securelist.ru

#Kaspersky
#BringontheFuture

www.kaspersky.ru

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER