«Лаборатория Касперского» провела оценку промышленной кибербезопасности для чешской пивоваренной компании Plzeňský Prazdroj

https://www.prazdroj.cz/en/

Plzeňský Prazdroj

Пивоваренный завод

- Основан в 1842 году
- г. Пльзен, Чешская Республика
- более 2000 сотрудников на 3 пивоваренных заводах и в 13 распределительных центрах
- 8 линий розлива на заводе в Пльзене

Plzeňský Prazdroj – чешская пивоваренная компания, основанная в 1842 году, с головным офисом в Пльзене, Чешская Республика.

Plzeňský Prazdroj – первая пивоваренная компания, начавшая производить светлое пиво низового брожения бренда Pilsner Urquell. Его оригинальная технология используется в производстве более чем двух третей выпускаемого сегодня в мире пива, в названии которого есть слово пилзнер, пилсенер или просто пилз. Название Plzeňský Prazdroj и Pilsner Urquell можно приблизительно перевести как «Подлинный источник Пилзнер».

Plzensky Prazdroj – ведущая пивоваренная компания в Центральной Европе. Под своими брендами Plzensky Prazdroj продает больше пива на чешском рынке, чем любая другая компания. С 1999 года пивоваренный завод являлся частью группы компаний SABMiller (в то время «Южноафриканские пивоваренные заводы»). В 2017 году Pilsner Urquell (за исключением отдельных географических регионов) был продан Asahi, ведущему производителю пива и безалкогольных напитков в Японии.

«Нам было очень важно подготовиться к любым неожиданным инцидентам, изучить нашу промышленную инфраструктуру и разработать план развертывания решения для обеспечения безопасности промышленной сети с помощью ведущих мировых экспертов»

Ян Шик,
главный инженер Plzeňský Prazdroj

Задача

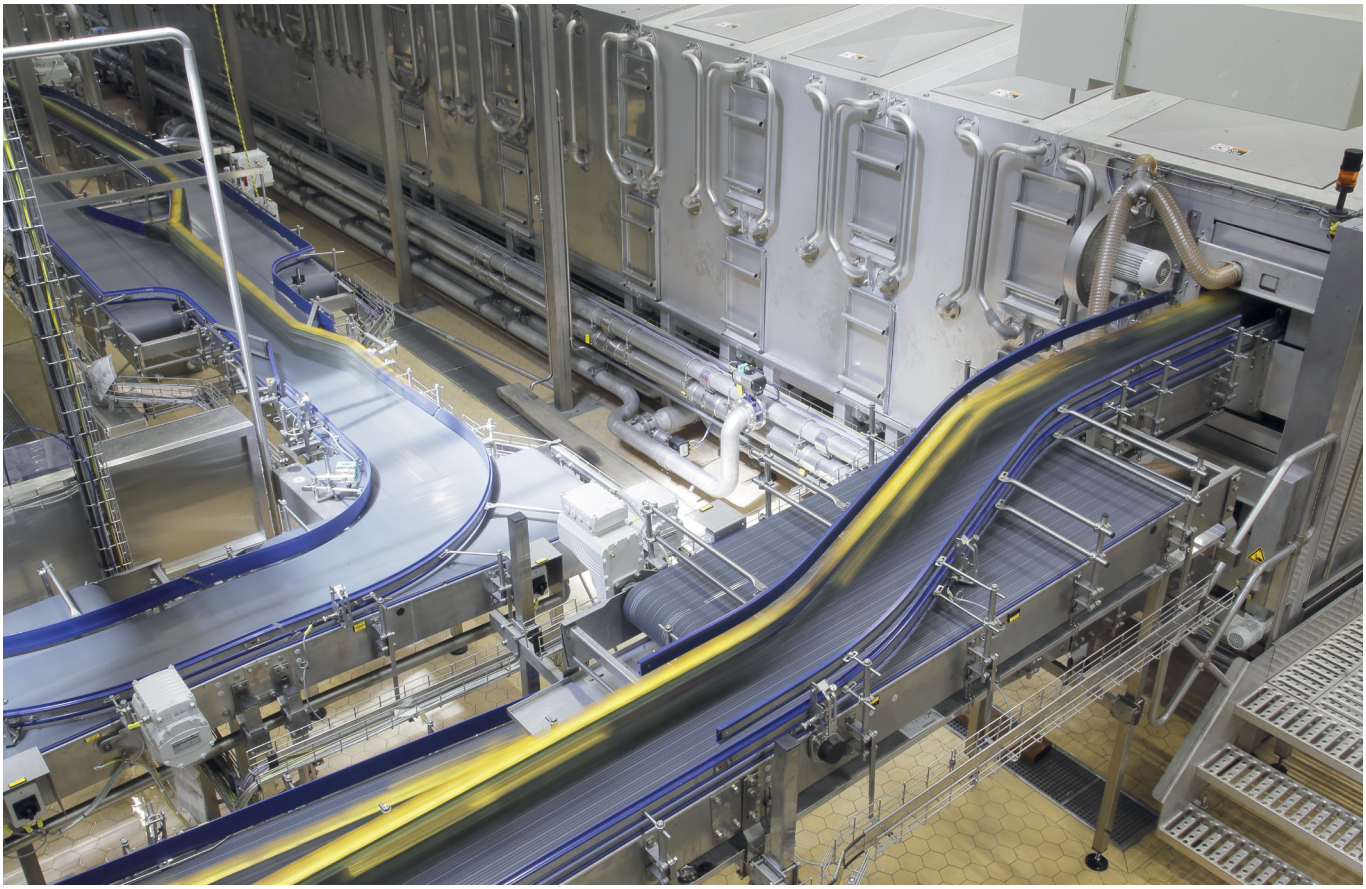
Как крупная промышленная компания, Plzeňský Prazdroj уделяет большое внимание кибербезопасности своих информационных и промышленных систем. За последние годы в компании было проведено несколько независимых проверок. А поскольку технологическое развитие на пивоваренном производстве Plzeňský Prazdroj является непрерывным процессом, возникла необходимость в новой независимой оценке защищенности промышленной среды.

В то время технологическая среда переводилась с отдельных систем, работающих на стандартных ПК, на виртуализированную серверную управляющую систему, объединяющую все системы и устройства.

Анализ защищенности (cybersecurity assessment, CSA) требовался прежде всего для проверки инфраструктуры на завершающем этапе проекта по виртуализации промышленных систем и модернизации основных компонентов промышленной сети. Также возникла необходимость в подготовке основных требований для будущего проекта по внедрению системы безопасности конечных узлов, а также в обеспечении защиты предприятий компании Plzeňský Prazdroj от целевых кибератак и от ущерба в случае успешной атаки на ресурсы компаний-партнеров.

Цель проекта по анализу защищенности заключалась в проверке надежности защиты от кибератак всех производственных линий и связанных с технологическим процессом программных и аппаратных средств, а также готовности компании к реализации целостной стратегии промышленной кибербезопасности.

Самыми трудными аспектами политик промышленной кибербезопасности до проведения CSA были сложность промышленной инфраструктуры (два сегмента - пивоварение и розлив - с двумя различными инфраструктурами), ее связь с внешними бизнес-системами и недавний запуск новой производственной линии.



Неинтрузивное решение
Анализ защищенности промышленных систем (Kaspersky Industrial CyberSecurity Assessment) не оказывает влияния на непрерывность технологических процессов.

Глубокая экспертиза
Реальный опыт работы с широким спектром отраслей и типов промышленного оборудования позволяет экспертам «Лаборатории Касперского» предоставлять эффективные сервисы по обеспечению промышленной кибербезопасности.

Комплексный подход
Kaspersky Industrial CyberSecurity - это набор технологий и сервисов, призванный помочь клиентам на всех этапах обеспечения безопасности промышленной среды: от обучения персонала и оценки защищенности до реагирования на инциденты.

Решение

Plzeňský Prazdroj обратился к «Лаборатории Касперского» для анализа защищенности промышленных систем (industrial CSA), который проводится экспертами компании удаленно или локально, с минимальным вмешательством в работу исследуемого предприятия.

Специалисты «Лаборатории Касперского» начали процесс CSA с аудита инфраструктуры и разработки модели угроз. Основные промышленные процессы в Plzeňský Prazdroj – пивоваренное производство и линии розлива. В общей сложности это 2 пивоваренных цеха, зоны цилиндро-конических танков и 8 линий розлива на заводе в Пльзене. Эксперты «Лаборатории Касперского» изучили наиболее критические сегменты инфраструктуры заказчика, имитируя определенные векторы атаки с целью обнаружения уязвимостей, вредоносной активности и различных аномалий.

Начав оценку с корпоративной сети, связанной с промышленной зоной, специалисты «Лаборатории Касперского» обнаружили, что установленное в ней бизнес-ПО сторонних производителей содержит опасные уязвимости, позволяющие киберпреступникам легко получить доступ к некоторым промышленным устройствам через другую IT-систему. В промышленном сегменте пивоваренной части производства специалисты «Лаборатории Касперского» обнаружили уязвимость нулевого дня в SCADA.

На этом этапе были также выполнены другие действия по обнаружению и описанию всех неконтролируемых входящих и исходящих внешних соединений с промышленной зоной.

«Решение о сотрудничестве с «Лабораторией Касперского» было принято нами легко по ряду причин. Мы высоко ценим их опыт в области обеспечения кибербезопасности промышленных систем, высокий профессионализм и комплексность их решения по сравнению с другими поставщиками. Всё это позволило создать благоприятные условия для развития целостной стратегии безопасности в нашей компании»

Ондрей Сикора,
менеджер C&A в Plzeňský Prazdroj

В завершение данного этапа CSA специалисты «Лаборатории Касперского» предоставили Plzeňský Prazdroj полный список обнаруженных уязвимостей и брешей в системе безопасности, включая слабую аутентификацию, SQL-инъекции и т. д., а также подробный анализ того, каким образом они могут быть использованы в преступных целях. Кроме того, Plzeňský Prazdroj получил описание обнаруженных и подтвержденных векторов атаки, которые могут привести к нарушению непрерывности и целостности технологических процессов компании.

Основываясь на данных исследований первых этапов, специалисты «Лаборатории Касперского» создали модель угроз, на базе которой был разработан список рекомендаций. Этот финальный отчет крайне важен для клиента, поскольку содержит рекомендации по мерам безопасности для отдельных промышленных компонентов и способам устранения обнаруженных уязвимостей. Рекомендации для Plzeňský Prazdroj включают обеспечение выполнения политик установки обновлений и использования паролей, а также повышение уровня безопасности локальной сети и веб-приложений.

«Анализ позволил нам получить важные рекомендации по жизненному циклу системы защиты и выявил слабые места в процессах обеспечения безопасности. Были определены области, требующие изменений, а все собранные данные были обобщены в финальном отчете», - сообщил Мирослав Заиц, IT-аналитик Plzeňský Prazdroj.

Перспективы

Plzeňský Prazdroj подтверждает, что специалисты «Лаборатории Касперского» профессионально организовали и выполнили анализ защищенности промышленной инфраструктуры и создали основу для стратегического подхода к обеспечению промышленной кибербезопасности внутри компании.

«Вместе с «Лабораторией Касперского» мы планируем следить за результатами оценки защищенности и выполнением полученных рекомендаций. Мы также продолжаем обсуждать развертывание решения Kaspersky Industry CyberSecurity для конечных узлов и серверов», - отметил Ондрей Сикора, менеджер C & A в Plzeňský Prazdroj.

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

www.kaspersky.ru
#ИстиннаяБезопасность

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* World Leading Internet Scientific and Technological Achievement Award at the 3rd World Internet Conference

** China International Industry Fair (CIIF) 2016 special prize