Тестирование на проникновение в АСУ ТП: «Лаборатория Касперского» способствует бизнес-росту компании Ezenta

ezenta

www.ezenta.com

Ezenta

Консалтинг в области информационной безопасности

- Год основания: 2000
- Главный офис: Херлев (Дания)
- Помогает датским государственным и коммерческим организациям, а также международным компаниям внедрять эффективные политики IT-безопасности.

Ezenta – одна из самых известных и уважаемых консалтинговых фирм Дании со специализацией в области информационной безопасности. Она помогает клиентам выстроить конкурентное преимущество на базе надежной платформы по защите промышленной инфраструктуры.

Ezenta не только оказывает профессиональные услуги, но и продает аппаратные и программные решения в области информационной безопасности. В штате компании работает всего 24 сотрудника, однако компания ежегодно генерирует валовой доход 19 млн крон (2,9 млн долл. США). В 2016 году ее прибыль после уплаты налогов составила 2,3 млн крон (345 тыс. долл. США).

«Найти экспертов в области промышленной кибербезопасности – задача непростая, так как это направление развития выбирают немногие».

Сёрен Эгеде Кнудсен, технический директор, Ezenta

Проблематика

Ezenta работает с АСУ ТП (автоматизированными системами управления технологическими процессами) с 2009 г. и накопила богатый опыт по защите промышленных инфраструктур. Стремясь развивать свой бизнес, Ezenta решила предложить клиентам сервис по тестированию промышленных систем безопасности на проникновение. В промышленной отрасли давно существует спрос на выявление уязвимостей в АСУ ТП: зная слабые места, можно ликвидировать бреши в системе безопасности, способные привести к простоям или еще более опасным последствиям. Однако сторонние консультанты, такие как Ezenta, при испытании АСУ ТП сталкиваются с трудностями, поскольку любая из этих систем требует уникального подхода и глубоких экспертных знаний.

Сотрудники Ezenta из группы по работе с АСУ ТП специализируются на традиционных аспектах информационной безопасности. Технический директор Сёрен Эгеде Кнудсен признает, что найти профессионалов с опытом работы в области промышленной кибербезопасности – задача непростая. Сотрудники Ezenta хорошо разбираются во многих тонкостях промышленной кибербезопасности, но им требовались дополнительные навыки для проведения тестирования на проникновение. Однако приобрести нужные навыки быстро и эффективно оказалось не так-то просто.

Компания, которая помогает клиентам повысить уровень безопасности АСУ ТП, должна превосходно разбираться в особенностях различных компонентов этих систем и находить особый подход к защите каждого из них. Для этого необходимо постоянное углубление имеющихся знаний и опыта в данной сфере.

Экспертные знания
Даже опытные профессионалы промышленной кибербезопасности сталкиваются с трудностями при переходе к ее новым аспектам – в частности, к тестированию АСУ ТП на проникновение.

Эффективный формат
Курсы Kaspersky Industrial CyberSecurity позволяют участникам в сжатые сроки научиться эффективно проводить тестирование на проникновение или приобрести навыки цифровой криминалистики в промышленных киберсредах. Все занятия основаны на реальных атаках, с которыми имели дело наши эксперты.

Новые возможности
Совместная работа с «Лабораторией Касперского» позволяет специалистам по кибербезопасности углубить свои знания в области АСУ ТП, а их компаниям – начать продажу и интеграцию высоко-специализированных технологий защиты.

Решение

С целью повысить квалификацию своих специалистов по АСУ ТП Ezenta решила внедрить программу обучения из портфолио Kaspersky Industrial CyberSecurity «Лаборатории Касперского», посвященную тестированию промышленных систем на проникновение. «“Лаборатория Касперского” прекрасно показала себя, передав нашим специалистам все необходимые навыки в области безопасности АСУ ТП. Курс обучения оставил только позитивные впечатления. Все тренеры обладали огромным опытом и солидными познаниями в промышленной кибербезопасности, были готовы ответить на любые вопросы», – рассказывает Сёрен Эгеде Кнудсен.

«Лаборатория Касперского» провела для сотрудников Ezenta трехдневный специализированный курс “Тестирование на проникновение в АСУ ТП для специалистов” из портфолио Kaspersky Industrial CyberSecurity, в ходе которого тренеры поделились знаниями и опытом во всех аспектах тестирования промышленных сред. Как правило, тестирование АСУ ТП на проникновение – очень непростой процесс с множеством нюансов. Прежде всего во время проверки специалисты по безопасности должны исключить простои или сбои производственного цикла. Благодаря отличному знанию операционных технологий, сотрудники «Лаборатории Касперского» смогли симулировать различные виды атак, основанные на реальных ситуациях, и разъяснить учащимся, как защитить промышленные компании от нападения такого рода. Более того, тренеры поделились с участниками курса ценным опытом по разработке экспертных рекомендаций для исправления уязвимостей и последствий атак, а также научили четко и последовательно анализировать результаты проверки.

«“Лаборатория Касперского” прекрасно показала себя, передав нашим специалистам все необходимые навыки в области безопасности АСУ ТП».

Сёрен Эгеде Кнудсен,
технический директор,
Ezenta

Результаты

Специалисты по безопасности АСУ ТП компании Ezenta приобрели необходимые им навыки и теперь могут самостоятельно проводить эффективные тестирования на проникновение в промышленных средах, а также давать клиентам рекомендации по устранению уязвимостей. По итогам плодотворного сотрудничества Ezenta обдумывает заключение долговременного партнерства с «Лабораторией Касперского».

«Ezenta планирует стать партнером “Лаборатории Касперского”, чтобы продвигать ее технологии и сервисы по обеспечению промышленной кибербезопасности на датском рынке», – сообщил Сёрен Эгеде Кнудсен.

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