ИСТОРИЯ УСПЕХА

ГК «Содружество» Аудит информационной безопасности

ГК «Содружество» – международная агропромышленная группа. Компания является вертикально интегрированной и состоит из четырех бизнес-единиц: перерабатывающие мощности (по производству белков и масел из растительного и животного сырья), торговля сельскохозяйственными товарами, специализированная инфраструктура (в т.ч. глубоководные морские порты) и логистика (в т.ч. железнодорожные и складские мощности).

Головной офис компании находится в Люксембурге, при этом компания владеет более чем 30 предприятиями, находящимися в 20 странах, в том числе в Бразилии, Парагвае, России, Турции, странах Средиземноморья и некоторых восточноевропейских государствах. Производственный комплекс ГК «Содружество» в Калининграде является одним из самых крупных предприятий по глубокой переработке семян масличных культур в России.

Аудит информационной безопасности охватил корпоративный сегмент информационной инфраструктуры, а также технологический сегмент – промышленные системы, обеспечивающие работу производственных цепочек от поставки сырья и переработки до отгрузки готовой продукции. Результаты проведения комплексного аудита позволили повысить общий уровень информационной безопасности предприятия, в том числе снизить риски нарушения доступности систем, что является принципиально важным для непрерывного производства. По итогам аудита была сформирована детальная Стратегия развития системы информационной безопасности заказчика в перспективе трех лет, включая расчет требуемых ресурсов.

«Мы хорошо понимаем, какова цена нарушения работы информационной или технологической системы предприятия в случае реализации угрозы ИБ, поэтому бизнес прямо заинтересован в повышении реальной защищенности. Мы поставили задачу выявить и нивелировать максимум возможных рисков. С учетом того, что инфраструктура предприятия является масштабной и сложной, а ландшафт угроз постоянно меняется, мы решили привлечь к этой работе профессиональных консультантов в сфере ИБ, которые обладали бы опытом защиты не только корпоративного, но и технологического сегмента. Эксперты компании "Инфосистемы Джет" помогли нам получить объективное представление об уровне защищенности наших систем, обнаружить уязвимости и оценить вероятность их эксплуатации злоумышленниками, а главное, выработать последовательность практических шагов по защите бизнеса от информационных угроз», – отмечает **директор ООО Управляющая компания «Содружество» Дмитрий Савенков**.

ОБЪЕКТЫ АУДИТА

ИТ-инфраструктура ГК «Содружество» является централизованной и обеспечивает работу всех филиалов компании в едином информационном поле. Ключевые информационные системы предприятия реализованы на единой платформе и логически связаны между собой, что обусловило широкие границы аудита.

В производственном сегменте предприятия эксплуатируется множество промышленных систем (АСУ ТП), отвечающих за различные звенья производственных цепочек. Аудит охватывал основные типы систем, функционирующих в рамках каждой конкретной производственной цепочки.

ЭТАПЫ ПРОЕКТА

Для получения максимально полной и объективной оценки текущего состояния информационных и промышленных систем был выполнен их комплексный аудит. Он включал в себя четыре основных этапа.

В рамках первого этапа было проведено обследование инфраструктуры и бизнес-процессов заказчика.

В ИТ-сегменте обследовались информационные системы и нижележащая ИТ-инфраструктура, сетевая инфраструктура, средства

Россия, 127015, Москва
ул. Б. Новодмитровская, д. 14, стр. 1
Тел.: +7 (495) 411-7601
Факс: +7 (495) 411-7602
E-mail: info@jet.msk.su
www.jet.msk.su

Андрей Янкин, заместитель директора Центра информационной безопасности компании «Инфосистемы Джет»:

«Активное содействие топ-менеджмента ГК “Содружество”, понимание ими важности выполняемых работ значительно способствовали успешной реализации проекта. Поскольку руководство было заинтересовано в объективном результате, мы оперативно получали исчерпывающую информацию и документы, необходимые для аудита, а также полное содействие со стороны сотрудников Компании. Данный проект – яркий пример совместной работы заказчика и исполнителя, направленной на обеспечение не “бумажной”, а реальной информационной безопасности, которая прямо влияет на стабильность функционирования бизнеса»

защиты, процессы, связанные с использованием информационных систем, а также процессы обеспечения ИБ. В качестве критериев оценки процессов управления и обеспечения ИБ использовались требования стандарта ISO/IEC 27001:2013. В процессе работ был проведен детальный GAP-анализ: оценка степени расхождения текущей ситуации в области информационной безопасности заказчика с требованиями ISO/IEC 27001:2013 с выработкой рекомендаций по достижению соответствия.

В технологическом сегменте были обследованы: оборудование промышленной сети, АРМ операторов, программные пакеты SCADA, система диспетчерского управления. При оценке степени защищенности эксперты руководствовались не только лучшими мировыми практиками, но и требованиями Приказа ФСТЭК России № 31 от 14.03.2014 г.

С помощью специализированных сканеров защищенности также была проведена проверка контроллеров АСУ ТП – на предмет актуальности прошивок оборудования, корректности установленных настроек безопасности и наличия уязвимостей.

По итогам первого этапа был составлен список рекомендуемых мер по устранению выявленных в результате обследования недостатков в системе обеспечения ИБ, а также обнаруженных уязвимостей.

На втором этапе эксперты провели качественный анализ рисков, основываясь на методике стандартов группы ISO/IEC 31000. Было проведено ранжирование рисков по степени критичности, определена очередность работ по их устранению.

В рамках третьего этапа проекта была выполнена серия пентестов внутренних ресурсов заказчика. Тесты на проникновение позволили подтвердить эксплуатируемость выявленных уязвимостей и недоработок, выявленных в рамках экспертного аудита. По итогам тестов был разработан ряд дополнительных рекомендаций по повышению защищенности информационных активов предприятия.

СТРАТЕГИЯ ИБ

Заключительным этапом проекта являлась разработка Стратегии информационной безопасности предприятия. Был определен целевой уровень ИБ в перспективе трех лет и построена «дорожная карта» перехода к целевому состоянию.

«Дорожная карта» включает в себя около 30 проектов, охватывающих разные аспекты повышения информационной безопасности на предприятии: совершенствование процессов обеспечения ИБ, внедрение дополнительных средств защиты, их настройку, разработку корпоративной документации в сфере ИБ, организационные изменения, в том числе, направленные на кадровое обеспечение поддержки системы информационной безопасности и т.п. Для каждого проекта были рассчитаны объемы необходимых ресурсов самого заказчика (финансовых, временных, кадровых), а также объемы привлекаемых ресурсов.

Стратегия одобрена заказчиком и принята к исполнению.